Reference Guide

hp StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Design

Product Version: 8.7P

Third Edition (March 2004)

Part Number: AA–RQ78C–TE

This document provides design assistance for HP customers, as well as for field and reseller presales technical support staff, for supportable HP StorageWorks Data Replication Manager solutions. This design guide provides help by discussing the different design tradeoffs and by providing a checklist of required solution hardware and software components, based on the results of the design process.

For the latest version of this reference guide and other Data Replication Manager documentation, access the website at http://h18000.www1.hp.com/products/sanworks/drm/index.html. Click the **technical documentation** link and the technical support page is displayed. Click **manuals (guides, supplements, addendums, etc)** for a listing of related documentation.

invent

Data Replication Manager HSG80 ACS Version 8.7P Design Reference Guide
Third Edition (March 2004)
Part Number: AA–RQ78C–TE

contents

Figures

Tables

About This Guide

This reference guide provides information to help you:

- Understand HP StorageWorks Data Replication Manager (DRM)
- Become familiar with design tradeoffs and considerations
- Plan configurations

This reference guide was reformatted with the information contained in the *HP StorageWorks HSG80 ACS Version 8.7P Data Replication Manager Design Guide Application Notes*. Minor edits have been incorporated due to changes in supported operating systems, links, and references.

"About this Guide" topics include:

Overview

This section covers the following topics:

- Intended Audience
- Related Documentation

Intended Audience

This document is intended for use by system and network administrators who are experienced in SAN fabric configurations and in planning disaster-tolerant solutions.

Related Documentation

In addition to this guide, HP provides additional information you may need to reference when connecting, configuring, and operating your DRM solution:

- *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Configuration Guide*, part number AA-RPHZF-TE
- *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Failover/Failback Procedures Guide*, part number AA-RPJ0E-TE
- *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Release Notes*, part number AA-RPJ2E-TE
- *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Scripting User Guide*, part number EK-DRMSC-OA. E01
- *HP StorageWorks Data Replication Manager Intersite Link Performance Analyzer*, part number AA-RV26A-TE
- *HP StorageWorks Continuous Access and Data Replication Manager SAN Extensions Reference Guide*, part number AA-RU5CE-TE
- *HP StorageWorks SAN Design Reference Guide*, part number AA-RMPNL-TE

Conventions

Conventions consist of the following:

- Document Conventions
- Text Symbols

Document Conventions

This document follows the conventions in Table 1.

Table 1: Document conventions

Convention	Element
Blue text: Figure 1	Cross-reference links
Bold	Menu items, buttons, and key, tab, and box names
Italics	Text emphasis and document titles in body text
`Monospace font`	User input, commands, code, file and directory names, and system responses (output and messages)
`Monospace, italic font`	Command-line and code variables
Blue underlined sans serif font text (http://www.hp.com)	Web site addresses

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings:

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Tip: Text in a tip provides additional help to readers by providing nonessential or optional techniques, procedures, or shortcuts.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site: http://www.hp.com.

HP Technical Support

Telephone numbers for worldwide technical support are listed on the following HP web site: http://www.hp.com/support/. From this web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Web Site

The HP web site has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com/country/us/eng/prodserv/storage.html. From this web site, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP web site for locations and telephone numbers: http://www.hp.com.

Data Replication Manager Overview

1

This chapter provides a description of the Data Replication Manager (DRM) solution and lists hardware and software that are supported.

This chapter consists of the following topics:

DRM Overview

DRM is a controller-based data replication software solution for disaster tolerance and data movement. DRM works with the HP StorageWorks Fibre Channel MA8000/EMA12000/EMA16000 and RA8000/ESA12000 storage systems.

DRM allows all data to be mirrored between storage elements in two different storage arrays that can be in separate geographical locations. Each write I/O is sent to both storage locations, and reads occur only at the local storage. Properly configured, DRM can be a complete disaster-tolerant storage solution that guarantees data integrity in case of a storage subsystem or site failure.

DRM copies data online and in real time to remote locations through a local or extended storage area network (SAN). For more information about devices used to extend the SAN, refer to the *HP StorageWorks Continuous Access and Data Replication Manager SAN Extensions Reference Guide.*

A basic DRM configuration is shown in Figure 1.

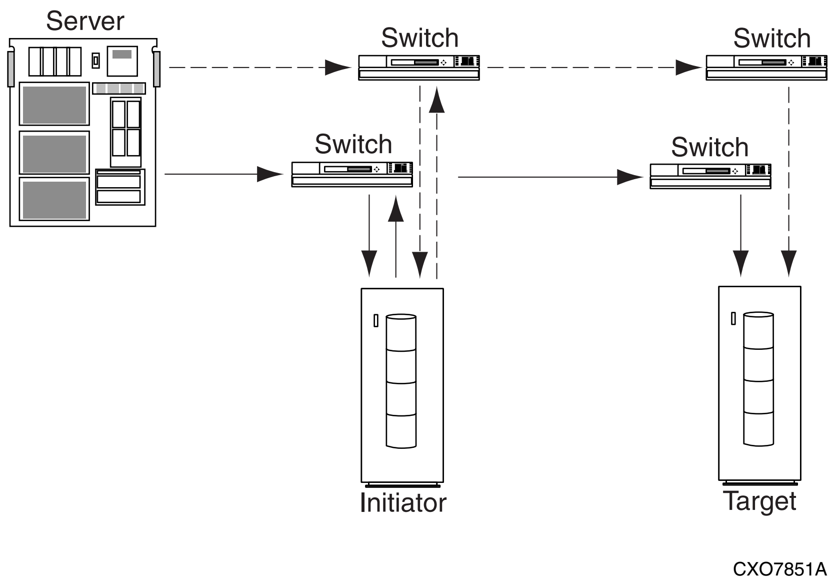

Figure 1: HP StorageWorks Data Replication Manager basic configuration

Supported Hardware and Software

Table 2 details the hardware and operating systems supported by DRM as of the time this document was published. Refer to the DRM Release Notes for a current list of supported hardware and operating system versions.

Table 2: DRM-Supported Host Servers/Operating Systems

Host Server	Supported Operating System
HP AlphaServer™	HP OpenVMS , HP Tru64 UNIX
HP ProLiant™ Server	Novell NetWare, Windows 2000, Windows NT
Hewlett-Packard HP9000—L, N, V Class	HP-UX
IBM—RS6000	AIX
Sun—Ultra SPARC	Solaris

Table 3 lists the supported operating systems by version and the SCSI command and control level that each operating system supports. Additional information on sharing of HP storage subsystems is available in the *HP StorageWorks SAN Design Reference Guide*. Other supported operating systems and specific versions are in the DRM Release Notes.

Table 3: DRM-Supported Operating System Versions

Operating System	Supported Version	SCSI-2 Support	SCSI-3 Support
HP HP-UX	v11.0 and 11.11 HP MC/Service Guard Clusters VA.11.14 Cluster Object Manager* Secure Path for HP-UX*	Yes	Yes
HP OpenVMS	v7.2-2 and 7.3 VMS Clusters appropriate to OS version	No	Yes
HP Tru64 UNIX	v5.1a and 5.1b TruClusters appropriate to OS version	Yes	Yes
IBM AIX	v4.3.3 & 5.1 HACMP Clusters* Secure Path for AIX*	Yes	Yes
Microsoft Windows 2000 for Server, Advanced Server, Datacenter Server	Service Packs 2, 3, and 4 MSCS* Secure Path for Windows*	Yes	Yes
Microsoft Windows NT Server	v4.0 Service Pack 6a with hotfix MSCS* Secure Path for Windows*	Yes	Yes
Novell NetWare	v5.1 and 6.0 Secure Path for Novell*	Yes	Yes
Sun Solaris	v2.6 (32-bit mode only) v7, v8, and v9 (32- and 64-bit mode) Secure Path for Sun* VERITAS Clusters* Sun Clusters*	Yes	Yes (v7 & v8) No (v2.6)
* Refer to the DRM Release Notes for the latest supported versions of these applications			

DRM supports the ability of compatible operating systems to share the same controller. To be compatible, all the operating systems must support the same level of SCSI command and control.

Design Tradeoffs

2

This chapter discusses tradeoffs that must be considered during the design of a Data Replication Manager (DRM) solution.

This chapter consists of the following topics:

Business Requirements

The first step in designing a data replication solution is to understand what is driving the need for it. In some cases, there is a business need for high availability, and disaster tolerance is seen as a side benefit. In other cases, there is a business requirement for disaster-tolerant data, with high availability of the applications being viewed as a side benefit. Neither type of configuration, however, satisfies both requirements without additional hardware or software. DRM provides disaster-tolerant data, while clustering technology (such as VMSClusters, TruClusters, Serviceguard Clusters, HACMP, MSCS, VERITAS Clusters, and Sun Clusters) supports high availability of applications. Together, these solutions provide highly available applications with disaster-tolerant data.

High Availability

DRM provides highly available and reliable access to data, but because it is a storage-centric solution, it does not provide highly available applications. To achieve highly available applications, standby servers are needed to provide the processing platforms used by the applications if the primary system fails.

Customers can deploy a cluster of servers at the primary site, with either a single backup server or cluster of servers at the remote site. The resulting configuration provides highly available and disaster-tolerant applications and data. In addition, DRM can function in both directions between sites to optimize the use of the equipment.

Table 4 shows the importance of high availability. Note that even at an availability of 99%, an application could be down for nearly 4 days per year.

Table 4: Real-world Availability: Outage Minutes per Year

Availability	90%	95%	99%	99.9%	99.99%	99.999%	100%
Approximate Outage Minutes per Year	50,000	25,000	5,000	500	50	5	0

Table 5 illustrates expected user outage minutes per year for several server types.

Table 5: User Outage Minutes and Relative Availability

	Windows NT Server	Windows NT Server & MSCS	Windows NT Server & MSCS & NonStop Software	NonStop Himalaya OS & NonStop Software
User Outage Minutes per User Year	8,200	3,150	1,150	180
Relative Availability	46 times less reliable than Himalaya	18 times less reliable than Himalaya	6 times less reliable than Himalaya	1x

Threat Radius

The threat radius is the distance from the center of a threat to the outside perimeter of that threat. For example, half the diameter of a hurricane or typhoon is the threat radius of that storm. Another example might be where a chemical factory is at the center of the threat radius circle. The threat radius is defined by the downwind distance of danger if there is a leak of hazardous chemicals.

The three general classes of threat in a DRM solution are local, within the metropolitan area, and regional. These three classes make it easier to characterize the solution in terms of intersite link options, performance, and system reliability. These three types of threats are defined as follows:

Local—Any threat that is less than a few kilometers in radius (less than 25 square kilometers), such as a tornado or a plant fire, is a local threat. Local replication has the least impact on performance as compared to the other options.

Metropolitan—Any threat that is larger than a local threat, and which might extend from 25 square kilometers to 5,000 square kilometers, such as a large chemical incident, a moderate earthquake, or a severe storm, is considered a metropolitan threat. Replication outside of metropolitan threats is similar in performance cost to running older disk drives—it is slower but acceptable.

Regional—Any disaster that affects a radius of hundreds of kilometers to tens of thousands of kilometers, such as a large flood or hurricane, is considered a regional disaster. By sheer size, the regional disaster requires the largest separation distance when planning disaster-tolerant solutions. Depending on the distances, data replication to the outside of a regional disaster threat radius will impact system performance. However, separation distances of more than 1,000 kilometers are rarely needed and only increase the cost of the link, rather than provide additional disaster tolerance.

In review, local disasters usually do not exceed a threat radius of a few kilometers. A metropolitan disaster covers threats with a radius greater than a few kilometers to tens of kilometers. The typical regional disaster covers hundreds of kilometers.

Examples of each disaster include:

- Building fire: local.
- Tornado: local, but possibly metropolitan if it stays on the ground for a long time.
- Hurricane/typhoon: metropolitan to regional, depending on size and intensity.
- Floods: local to regional along the flood plain.
- Earthquake: usually local to metropolitan, depending on severity.
- Environmental: local.
- Power loss: local to regional, depending on which component fails—a local distribution point or a major portion of the regional power grid.

In considering the threat radius, planners must decide what the threats are to the primary system, and whether those threats also apply to the backup system. For example, it would be unwise to place both sites in the same flood plain because one flood could destroy both. Similarly, if severe storms tend to travel in a certain direction, then a good strategy would be to place the two sites perpendicular to the expected route of travel and as far apart as possible to prevent one storm from affecting both sites.

Figure 2 is an example of the relative relationship between the three classes of threats based on the radius of those threats.

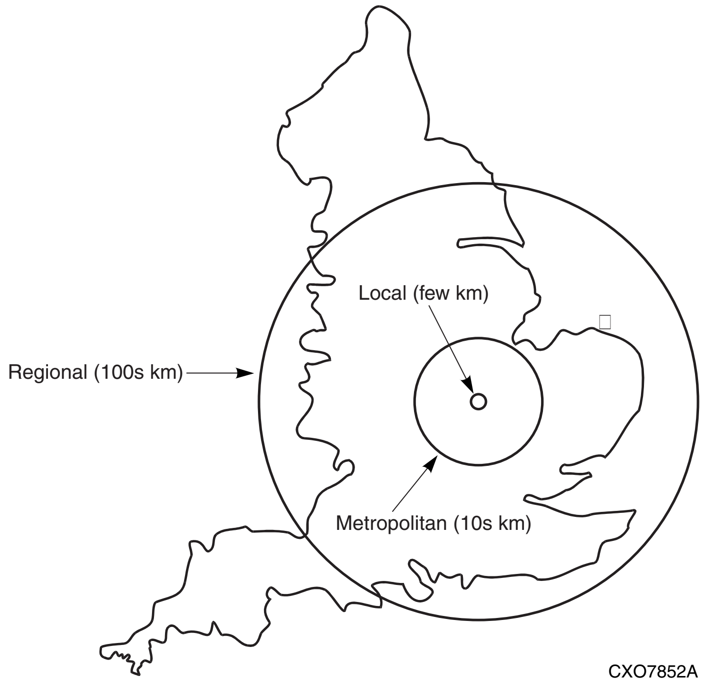

Figure 2: Threat radius

Disaster Tolerance

Disaster tolerance is the ability of a system to withstand a defined disaster, such as being outside the threat radius for that potential disaster. DRM enables applications to automatically and continuously build two copies of application data at geographically separated sites.

The larger the potential disaster (threat radius), the farther apart the primary and backup sites need to be. To determine an adequate distance, first determine what kinds of disasters are probable in the local area and understand the protection distances needed to separate the two sites. Consider any local regulatory requirements that might increase or limit the separation distance. For example, some counties in the United States require both sites to remain within the same 100 to 400 square-kilometer county. This restriction has limited the maximum separation distance to less than 30 km in an area prone to earthquakes. Such earthquakes have impacted buildings several hundred kilometers from the earthquake epicenter.

On the east coast of the United States, and the southern and eastern coasts of the Asian subcontinent, hurricanes or typhoons can cover an area with a radius of 200 km or more. Other natural disasters include regional forest fires, localized tornadoes, and widespread flooding. Non-natural disasters include building fires or chemical contamination, either of which can limit access to computer facilities.

In order to deal with the types and scope of potential disasters, storage system planners must consider the inherent tradeoff—with increasing distance comes lower performance.

Physics of Distance

A data replication product can move data at extreme distances, but due to propagation delays inherent in data transfers, it may take a long time for each replication I/O to be completed. The distance between the two sites, not the width of the pipe, is the limiting factor in replication performance. This section provides a brief overview of the impact of distance on the sustainable I/O rate.

In Figure 3 there are two I/O pipes: one narrow arrow representing a slow communications channel, and a wider arrow representing a high-speed intersite link. Both I/O packets (shown by the parallelograms) contain the same amount of data. They are moving from Site A to Site B (left to right), and the leading edge of both will arrive at Site B at the same time. The difference in pipe size (bandwidth of the link) allows the faster pipe to complete delivery of the packet before the slower pipe. The difference is that the wider pipe provides shorter times to load and unload the packet. At long distances, the communications bandwidth becomes a less important factor in determining the I/O rate.

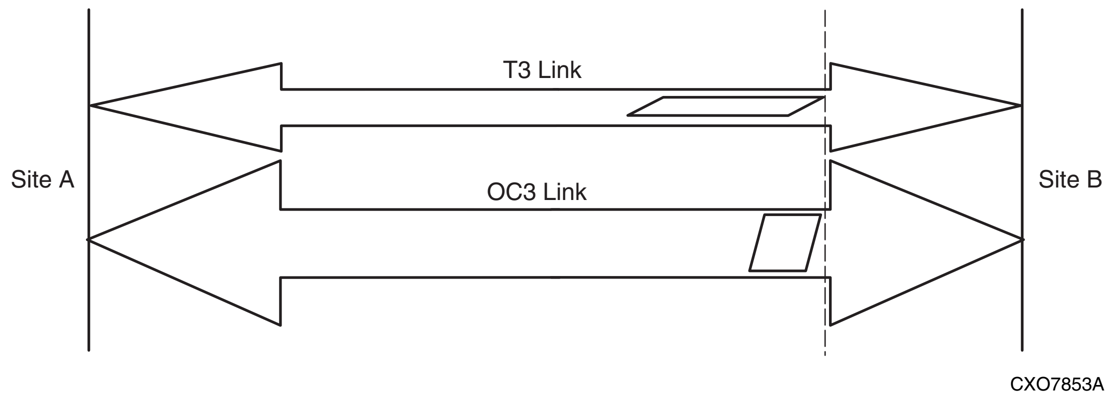

Figure 3: Impact of distance on I/O rate

The time required to load or unload a packet can be approximated using the bandwidth of the pipe and the size of the packet. For example, given a 16-KB packet and a T1 transmission speed of 1.54 Mbps, it takes approximately 0.1 seconds to load the packet onto the link. Using a Fibre Channel link running at 1,000 Mbps and the same 16-KB data packet, the time is reduced to 0.00016 seconds.

Table 6 provides the data for calculating how long it takes to complete a single I/O across a zero distance intersite link, based on the link bandwidth and the size of the data packet. The columns are the transmission technology, performance or bandwidth of common intersite links, the slope *m* of the line that approximates the time it takes to load the data onto a given pipe, and the Y-intercept *b* representing the replication and conversion overhead.

Enter the size of the data packet *X* in kilobytes and calculate the zero distance I/O completion times *Y* as follows:

Y (in milliseconds) = $mX+b$

Note that intercept *b* represents the minimum amount of time it takes to load one 512-byte data packet onto the intersite link. In addition, the slope *m* of the line represents the amount of additional time it takes to insert ever larger data packets onto the intersite link.

Table 6: Link Performance Table

Intersite Link Technology	Intersite Link Bandwidth (Mbps)	Slope (m)	Intercept (b)
Fibre Channel	1000	0.056	0.84
1-GbE (Gigabit Ethernet) IP	1000	0.056	0.84
OC3-ATM	155	0.134	1.8
100-Mbit IP	100	0.134	1.8
100-Mbit IP with very high compression	100	0.056	0.84
T3-ATM	44	0.32	2.8
10-Mbit IP	10	1.02	3.0
10-Mbit IP with very high compression	10	0.134	1.8

Note: m = a number proportional to the amount of time it takes to send larger packets versus smaller packets.

b = the replication overhead—the amount of time it takes to replicate one 512-byte block.

The second factor in determining how long it takes to complete a single I/O over distance is the time it takes for the leading edge of the data to travel from one end of the link to the other. This time can be estimated using a speed of 200,000,000 m/s for light in standard fiber-optic cable, which equates to 5 microseconds per kilometer. For an intersite separation distance of 10,000 km, the time interval would be 50,000 microseconds or 0.05 seconds, and is 25 times the average rotational latency of a 15,000 rpm disk drive (which is 0.002 seconds).

DRM implementation of the FC-defined SCSI protocol requires four trips through the intersite link to complete a single write. First, the SCSI initiator must ask the SCSI target if it is ready to accept data. Second, the SCSI target indicates it is ready. Then, the SCSI initiator sends the data to the target. The final trip occurs when the SCSI target replies that it has received the data. The true time it takes to move data from the initiator controller to the target controller is four times the single-trip distance, plus the time it takes to load the data for a given pipe size. These four trips, consisting of three small control packets and one large data packet, equate to 20 microseconds of latency per kilometer of intersite link distance to complete the SCSI write. Based on the distance between the two sites, this latency is added to the previously calculated time to complete a zero distance I/O.

Two methods are used to calculate the intersite latency based on the cable distance between the two sites. One is based on the driving distance, the other on the network latency. If an intersite network exists, use the more accurate network latency as the metric. If an intersite network does not exist, then use the driving distance approach.

Driving Distance

To estimate the cable distance between two sites, measure the distance by driving a car between the two sites. For point-to-point networks, multiply the driving distance by 1.5. For routed networks, multiply the driving distance by 2.25. For example, if two sites are located 150 km apart, the estimated cable distance for a point-to-point network would be 225 km.

Network Latency

If an intersite network connection exists, ask the network engineers for an estimate of the one-way or round-trip intersite latency. In the preceding example, the actual point-to-point network was measured to give one-way latency of approximately 5 milliseconds or 250 km, instead of the 225 km originally estimated by using driving distance.

Single Stream I/O Example

DRM invokes a process called *normalization* whenever a *remote copy set (RCS)* is created. The remote copy set function allows data to be copied (mirrored) from the initiator site to a target site. The result is mirrored data at two disparate sites. During the normalization process, data is copied from the initiator side of the logical unit to the target side of the RCS. Each write copies 128 blocks of 512 bytes (or 64 KB of data) from the initiator to the target. To prevent overwhelming the system, only one write per RCS is allowed to be outstanding. This is defined as a *single synchronous I/O stream*.

For the purpose of this example, assume that the two sites are located 100 km apart and that the RCS consists of two 9-GB disk drives, one at each site.

Table 7 provides the calculation results for loading 64 kilobytes of data onto the different links.

Table 7: Calculation of Time to Load Data onto an Intersite Link

Technology	Slope	Time to Load 64 KB of Data (ms)
Direct FC or GbE	0.056	3.58
FC/ATM OC-3 or 100 Mbps	0.134	8.58
FC/ATM T3	0.32	20.48
FC/IP 10-Mbit with no compression	1.02	65.28

Given the intersite distance of 100 km, the transfer latency is 100 x 20 microseconds/km = 2 milliseconds, and is approximately the same for all interconnects.

Table 8 provides the calculation for adding the two results together, plus the replication overhead.

Table 8: Calculation Time to Complete a Single I/O Over Distance

Technology	Time to Load (ms)	+ Intersite Latency (ms)	+ Overhead (ms)	= Time to Complete I/O (ms)
Direct FC or GbE	3.58	2	0.84	6.42
FC/ATM OC-3 or 100 Mbps	8.58	2	1.8	12.38
FC/ATM T3	20.48	2	2.8	25.28
FC/IP 10 Mbps	65.28	2	3.0	70.28

Inverting the time-to-complete number (milliseconds per I/O) produces an approximate number of single-stream synchronous writes that can be completed every second for the various bandwidths of pipes for the example distance. The results are shown in Table 9 as approximate times needed to normalize a 9-GB logical unit number (LUN).

Table 9: Relationship of I/O Per Second to Throughput and Time to Normalize a 9-GB LUN

Technology	Approximate I/O per Second	Throughput (Based on 64KB per I/O)	Approximate Time Required to Normalize a 9-GB LUN
Direct FC or GbE	155.7	35.87 GB per hour	0.25 hour
FC/ATM OC-3 or 100 Mbps	80.8	18.62 GB per hour	0.48 hour
FC/ATM T3	39.6	9.11 GB per hour	0.98 hour
FC/IP 10 Mbps	14.2	3.28 GB per hour	2.75 hours

You can also use the *HP StorageWorks Data Replication Manager Intersite Link Performance Analyzer Calculation Tool* to perform these same calculations.

Multiple I/O Streams for a Single Application

After determining the worst case for the time duration to perform the replication of a single write, you must examine the impact of multiple I/O streams from a single application. Multiple writes can be replicated at the same time, as shown in Figure 4. The wider the pipe, the more writes it can hold, up to a maximum called the bandwidth-latency product. Multiply the net performance of the communications pipe (total bits per second, less any overhead) times the intersite latency in seconds. This number, when expressed in bytes (use 10 bits per byte) and divided by the average message size (in bytes), determines the average number of messages that can be in the communications pipe at one time.

In Figure 4, the parallelograms represent two I/O streams. Each I/O stream consists of data packets of equal size (same number of bytes). The narrow pipe is able to hold only three packets, but the wider pipe is able to hold nine packets.

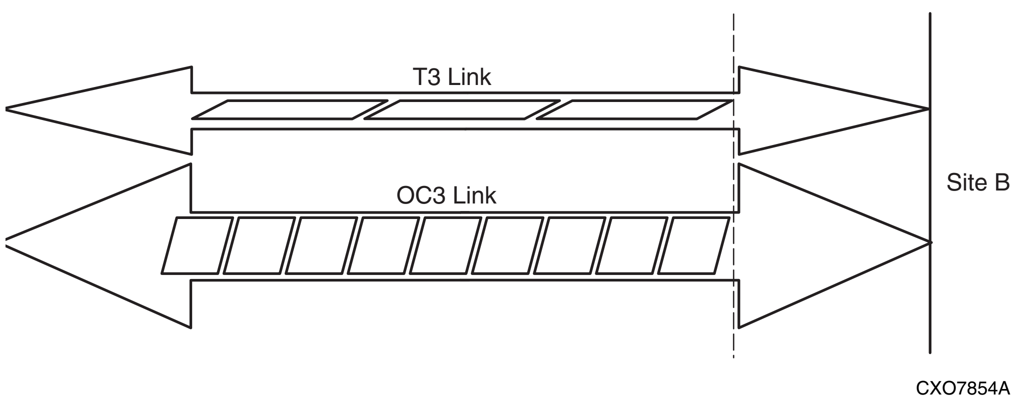

Figure 4: The impact of multiple I/O streaming for single applications

Two other constraints will further limit the maximum number of I/O streams in the pipe. The first limit is the number of Fibre Channel buffer-to-buffer credits allowed between any Fibre Channel devices. For example, using B-series Fibre Channel switches running any version 2 firmware, this number is currently defaulted at 16, for 16 open message exchanges. This limit is seen on any long distance direct Fibre Channel connection with very long distance gigabit interface converters (GBICs) or wavelength division multiplexing (WDM) solution. It is not usually seen in DRM-over-ATM or DRM-over-IP because the credit is returned by the ATM or IP gateway to the sending switch.

The second limit is the maximum number of outstanding I/Os the HSG80 controller can support. At any one time the HSG80 controller allows up to 240 outstanding synchronous write I/Os. If the bandwidth latency product of the link can support more than 240 I/Os, such as in high speed, very long distance DRM-over-ATM or DRM-over-IP configurations, then the maximum number of I/Os outstanding in the pipe will be 240 per pair of HSG80 controllers sharing the same pipe.

Multiple I/O Streams for Multiple Applications

The same limitations shown in Figure 4 apply to situations where multiple I/O streams are issued by multiple applications (Figure 5). Any differences in the number of I/Os in the pipe are based on how the I/O bandwidth is shared between the competing applications.

Within the controller, each remote copy set can share the total outstanding I/O. The default per remote copy set is 200. Although it can be increased to 240, there is the potential for one high performance application to take all 240 I/Os, which slows the other remote copy sets.

If there are multiple high performance applications, then best practice is to add more pairs of DRM storage arrays to maintain performance. The bidirectional solution discussed later in this document is one configuration option for maintaining performance.

In no case should the average loading on any link exceed 40% of its rated capacity, and the peak loading should not exceed 45% of rated capacity. This limitation allows an I/O from a failed link or fabric to run on the nonfailed fabric or link without causing additional failures due to overloading of the surviving fabric.

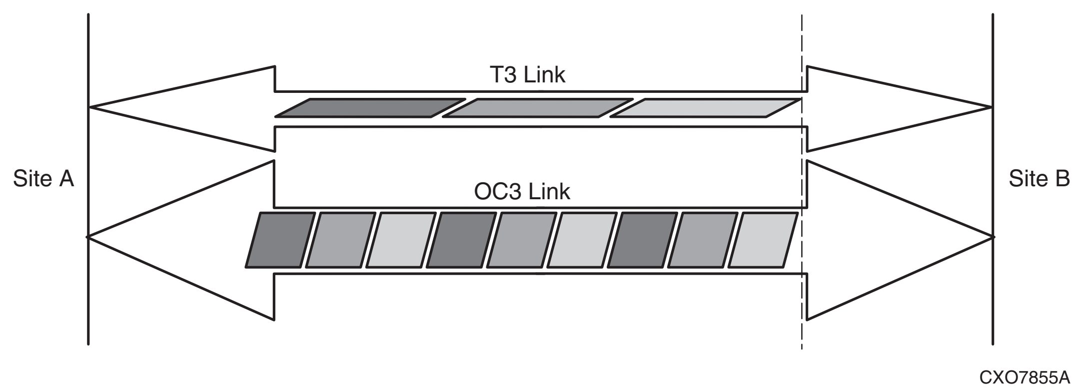

Figure 5: The impact of multiple I/O streaming for multiple applications

Trunking

Third generation Fibre Channel switches or later operate at 2 Gb per second and enable a feature called *trunking*. Trunking is the combining of two or more low-speed intersite links (ISLs) into one virtual high-speed ISL, thereby increasing link performance. Trunking is supported for ACS Versions 8.6 and 8.7, and is automatically enabled by the switches when more than one ISL exists.

Synchronous versus Asynchronous Replication

There are two methods for replicating data: synchronously or asynchronously. A possible third way, semi-synchronously, is really a controlled asynchronous solution.

In DRM synchronous replication, the write I/O is sent to both the local and the remote site for near-simultaneous writes to disk. After the data from that write request or the write I/O itself has been moved to both locations, an acknowledgment is sent back to the requesting application. If one of the two writes fails, then depending on error conditions, the application is sent an aborted I/O response.

Within DRM, this failsafe error mode prevents completion of an I/O if either of the storage controllers is unavailable. Therefore, only writes that are completed at both sites are acknowledged, and both data sets are always in synchronization from the perspective of the application and its completed transactions.

In asynchronous replication, the write I/O need only be completed on the local storage controller before it is acknowledged as complete. Then the replication occurs and the I/O is completed at the remote site. The size of the queue determines the maximum length of time between the local and remote writes.

Asynchronous replication puts in jeopardy any data that is in the queue and not yet replicated to the remote site. The data in the queues appear as completed transactions from the perspective of the application, but the data may never reach the replication site if the primary site fails with the data still in the queue.

DRM supports both synchronous and asynchronous replication of the write I/O. Figure 6 shows the relative performance differences between synchronous and asynchronous replications. The vertical axis is the response time, or time it takes to complete a single I/O over distance for the two types of replication. The horizontal axis is the relative I/O rate for a given separation distance. Only where the application I/O rate is below saturation (as shown in the shaded area) will asynchronous replication respond faster than synchronous replication. In all other cases, and in all DRM solutions tested to date, synchronous replication is the recommended solution.

Note: Because actual values depend on the size of the I/O and the intersite distance, only the relative relationship between response time and I/O rate is shown in Figure 6.

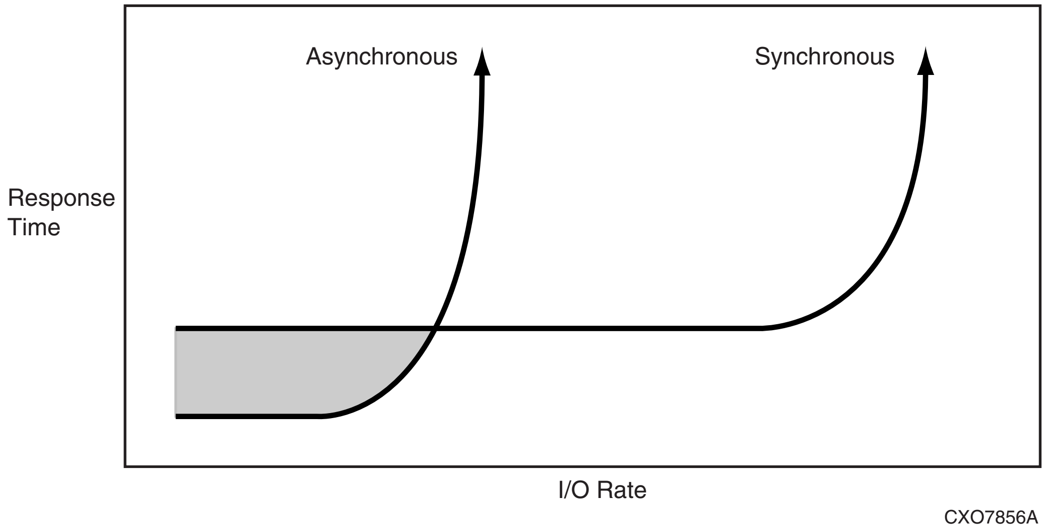

Figure 6: Asynchronous versus synchronous replication

The asynchronous response curve saturates well before the synchronous response curve. It takes more processing time to complete an asynchronous I/O because of the need to load the data into the queue, maintain the queue, and then remove the I/O from the queue. Inverting the time it takes to process one I/O yields the approximate I/O rate, which for asynchronous transfers is lower than that for synchronous transfers. Only by combining multiple transactions into one intersite data transfer can this limit be removed, but doing so places even more data in jeopardy if the link to the secondary site fails.

Bidirectional Solution

Another DRM tradeoff is the direction of the transfer versus intersite link pipe size. Because data is moving in both directions simultaneously, the increased data traffic may require higher bandwidth data pipes until the data reconstruction process is completed.

Determine if the business needs can support bidirectional data transfers. Bidirectional data transfer keeps both sites active and allows them to back up each other in case of a disaster. In DRM, the storage must be either the initiator of the replication or the target of the replication.

Bidirectional replication also can be configured so that servers at the remote site, while performing secondary tasks, are ready to support the primary applications if the primary site is damaged. Also, the remote site servers can be set up to handle some of the primary site application load, if the application load is easily divided. Secondary tasks that the remote site can perform include backup, generating reports, or data mining.

To establish a bidirectional solution, calculate the maximum I/O rates needed for each direction. This calculation is used to ensure that the I/O pipe is wide enough to handle the workload of both sites while in a degraded or failed condition. The diagram in Figure 7 shows one bidirectional solution.

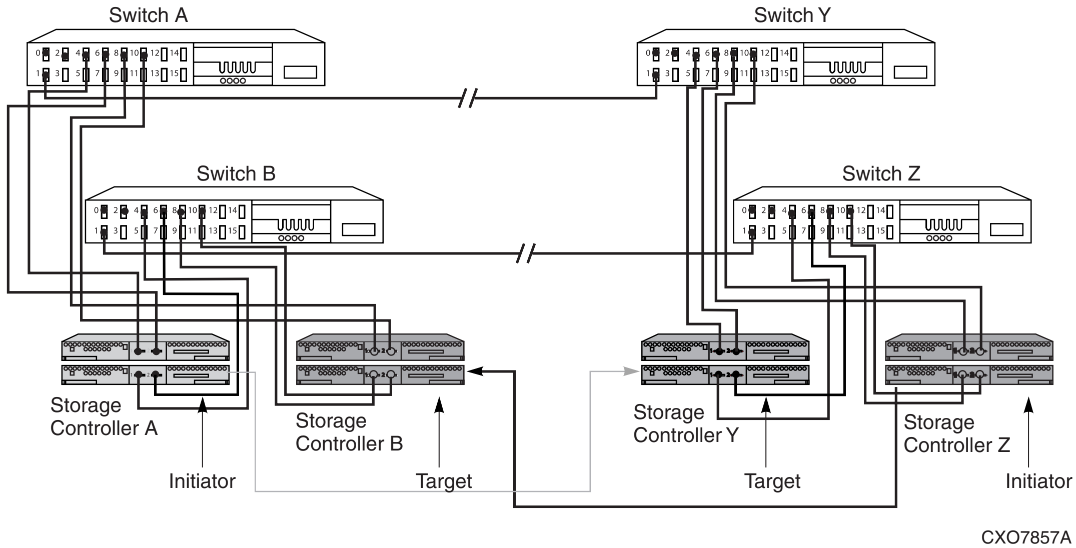

Figure 7: Bidirectional DRM solution

Determining Write-to-Disk Rate

For existing applications, determine the current I/O performance rates for each disk that is to be replicated to the remote site. Finding the average and maximum write rate (write I/O per second) and peak write transfer rate (bytes per second) may require some analysis and time. Operating system-specific tools, such as *PERFMON* or *IOSTAT*, can be used to collect the data. The HSG80 performance monitoring tool *DSTAT* can also be used to monitor controller workloads. If the data is available only as an average over time, attempt to ascertain the peak hours of operation and estimate the peak write rate and write transfer rates.

Record the peak and average write rates and write transfer rates and, if bidirectional, record these numbers for each direction. Compare these numbers to potential intersite links and see if the link technology is affordable. If not, look at other ways to replicate the data or replicate only the most critical data, such as transactions or redo logs.

In no case should the average loading on any link exceed 40% of rated capacity, and the peak loading must not exceed 45% of rated capacity. This limitation allows I/O from a failed link or fabric to run on the nonfailed fabric or link without also causing additional failures of the surviving fabric.

DRM Storage Design Considerations

3

This chapter describes storage array design considerations that you need to understand before you design a Data Replication Manager (DRM) solution.

This chapter consists of the following topics:

Disaster-Tolerant LUNs

A single DRM-based pair of storage arrays supports a maximum of 12 remote copy sets (RCSs), where an RCS is a logical storage unit that is to be replicated to the remote site. Although 12 are supported, there are also reasons for not using all the available RCSs in an array. For example, an application can generate multiple I/O streams using the entire I/O bandwidth of the controller and only require five RCSs. Also, the size of a single storage set might require most of the available drives within the storage array cabinet. Finally, some smaller DRM installations may not need all 12 RCSs. Each RCS can exist in any supported JBOD, RAID-0, RAID-1, RAID-0+1, or RAID-3/5 format. Both sites must contain the same size and geometry to facilitate failover and failback operations.

On a worksheet, record the number, RAID type, and raw size of each remote copy set. Use this data to determine the number of storage arrays, disk drives, and so on that will be needed to build the solution at both sites.

Non-Disaster-Tolerant LUNs

A DRM-based storage array can also provide nonreplicated (non-disaster-tolerant) storage sets. These sets of disks are not replicated to the remote site and can be used for almost any purpose. For example, at the DRM initiator, each RCS can be cloned as a point-in-time copy. The clones are stored in the non-RCS storage sets. Similarly, at the target site, a clone or snapshot of each DRM remote copy set target can be taken. The non-RCS at the target is used to store the clones or snapshots.

Finally, the non-RCS storage set can be used for temporary or scratch space. Each non-RCS storage set can exist in any supported JBOD, RAID-0, RAID-1, RAID-0+1, or RAID-3/5 format. Due to the impact on performance, HP does not recommend placing the page/swap file on a storage controller that is also performing data replication.

Non-disaster-tolerant storage sets also can be used for offsite backup. Remote vaulting of the replicated data is accomplished by first taking a snapshot of the data and then using a standby server to move the data from the snapshot to the backup media. This process occurs at the remote site, but having the data onsite ensures faster restores by the storage array network back to the primary site.

Up to four active snap volumes per pair of HSG80 controllers are supported at any point in time. Each snap volume must be at least as large as the source volume, and larger if it is to be written to. Because a snap may be reused, it should be at least as large as the largest possible source volume. The number of cloned storage sets is limited to the total number of storage sets supported in the array. During cloning operations, the maximum number is limited by the total number of mirrorsets shown in the following section.

Array Limits

In addition to the limit of 12 RCSs, each array (pair of controllers) is also limited to the following:

- 24 visible LUNs (12 RCS and 12 non-RCS LUNs)
- Maximum 1.024 TB storageset size. Minimum size is one drive.
- 92 (96 minus 4) peer-to-peer host connections
- 20 RAID-3/5 storage sets
- Combined maximum of 30 RAID-1 plus RAID-3/5 storage sets (no more than 20 RAID-3/5 storagesets)
- Combined maximum of 45 RAID-0, RAID-1, plus RAID-3/5 storage sets (no more than 20 RAID-3/5 storagesets)
- 8 partitions of a non-RCS storageset or individual disk
- 6 physical devices per RAID-1 storageset (mirrorset)
- 14 devices per RAID-3/5 storageset (RAIDset)
- 24 devices per RAID-0 storageset (stripeset)
- 45 devices per RAID-0+1 storageset (striped mirrorset)

A remotely mirrored storageset (remote copy set) device array cannot be partitioned by the array controller. Verify that these limits do not impact any of the preceding calculations. If they do, then add more storage arrays or reconsider how the storage can be configured so that none of these limits are exceeded.

An RA8000/EMA12000 is limited to 72 drives, an MA8000 is limited to 42 drives, and an ESA12000 is limited to 60 or 84 drives, depending on type. The EMA16000 is limited to 42 drives per controller pair, or 168 drives total. A variation of the EMA16000 contains 2 controller pairs and accommodates 84 drives total.

Fabric Port Count Results

The final tradeoff to consider is the number of controller pairs and the number of servers used by the applications. At this writing, the maximum size of a SAN is limited to 28 B-series (or 11 C-series or 24 M-series) switches per fabric. In DRM there are two fabrics and two sites, meaning a total of 56 B-series switches split between the two fabrics and two sites. These switches are distributed across the fabrics in one of several topologies, as described in the *HP StorageWorks SAN Design Reference Guide*. This reference guide also lists the limitations for each type of Fibre Channel switch.

The SAN design limit of 28 B-series switches per fabric allows for a maximum of over 700 device ports. These ports are consumed on each fabric at the rate of one port per host bus adapter (HBA) pair and two ports per controller pair. Using B-series switches, the initiator controller should be located no farther than seven switch-to-switch hops from the server issuing the I/O. The target controller should be located no more than seven switch-to-switch hops from the initiator. With C- and M-series switches the number of hops is limited to three.

To determine the number of open ports required for the solution, add the number of HBA and controller ports on each fabric at each site. Each controller has two ports per fabric, while each HBA has only one. Therefore, you also must total the storage and the switch ports (per fabric) required for each site and record the numbers on your worksheet. Remember to account for all interswitch and intersite links when determining the number of open ports available for a given fabric topology.

Failover Requirements Planning

The following sections describe timing guidelines to consider when performing initial failover and failback processing.

Planned Failover Event Time Limits

Decide whether you want to periodically fail over to the remote site for role reversal. For example, assume that the primary database administrator (DBA) is at the primary site, the alternate DBA is at the alternate site, and the primary DBA is going on vacation. You can use DRM to move the database temporarily from the primary site to the alternate site. This move is supported with the role-reversal procedure documented in the *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Failover/Failback Procedures Guide*.

DRM does not support more than four failover or failback events per hour. Worst-case testing has shown that it usually takes less than 30 minutes to manually perform a failover or failback operation. Best-case testing with scripting has shown a processing time of about one minute, depending on the number of remote copy sets involved. Add to these times the time it takes to restart the application to determine the approximate failover and failback times and ensure that these calculated times are within scope of the business requirements. Refer to the *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Failover/Failback Procedures Guide* for more information.

Unplanned Failover Event Time Limits

Several options exist within the DRM solution for managing either the planned or unplanned failover and failback events. At present, failover and failback events can be either manual or automated, but none are automatic. When designing these limits, the longest part of the process may not be the failover of the storage but rather the restarting of the application that uses the storage. Therefore, use caution when specifying maximum failover times. For the fastest and most accurate failover or failback process, use the DRM *scripting* utility. By using scripts, you can automate the process and greatly reduce the need for CLI commands. After you have set up your scripting configuration, you run the scripts, which issue the appropriate CLI commands. By using one scripting program file, you can start a complete failover or failback sequence. For more information on scripting, refer to the *HP StorageWorks Data Replication Manager HSG80 ACS Version 8.7P Scripting User Guide*.

DRM does not support automatic site failover or failback at this time. Human intervention is often needed in catastrophic failure situations because of limitations on automatic failover management tools. For example, during a multiple link failure that causes total site isolation, some automatic tools will start the failover process due to isolation from the primary site, but the primary site may still be processing locally generated transactions. You can assess these factors and delay the failover in order to avoid local data corruption. For more information, refer to the *Disaster Recovery Journal* at:

http://www.drj.com

DRM Configurations

4

This chapter describes different Data Replication Manager (DRM) configurations.

This chapter consists of the following topics:

Basic DRM-over-Fiber

DRM-over-fiber is the most basic of the DRM configurations, and all others build upon it. As shown in Figure 8, the cabling in this configuration supports two redundant fabrics, where the first HBA in host A is connected to switch A and the second HBA in host A is connected to switch B. The top controller of the initiator controller pair is also attached to switch A, and the bottom controller is attached to switch B. At the target site on the right side of the figure, the backup server and the target storage array are wired the same way as at the initiator site. Use the same switch ports for the same functions at both sites to reduce confusion during a disaster or debugging. HP also recommends naming the two fabrics to distinguish them. For example, you might name them TOP/BOTTOM, RED/BLUE, and so on.

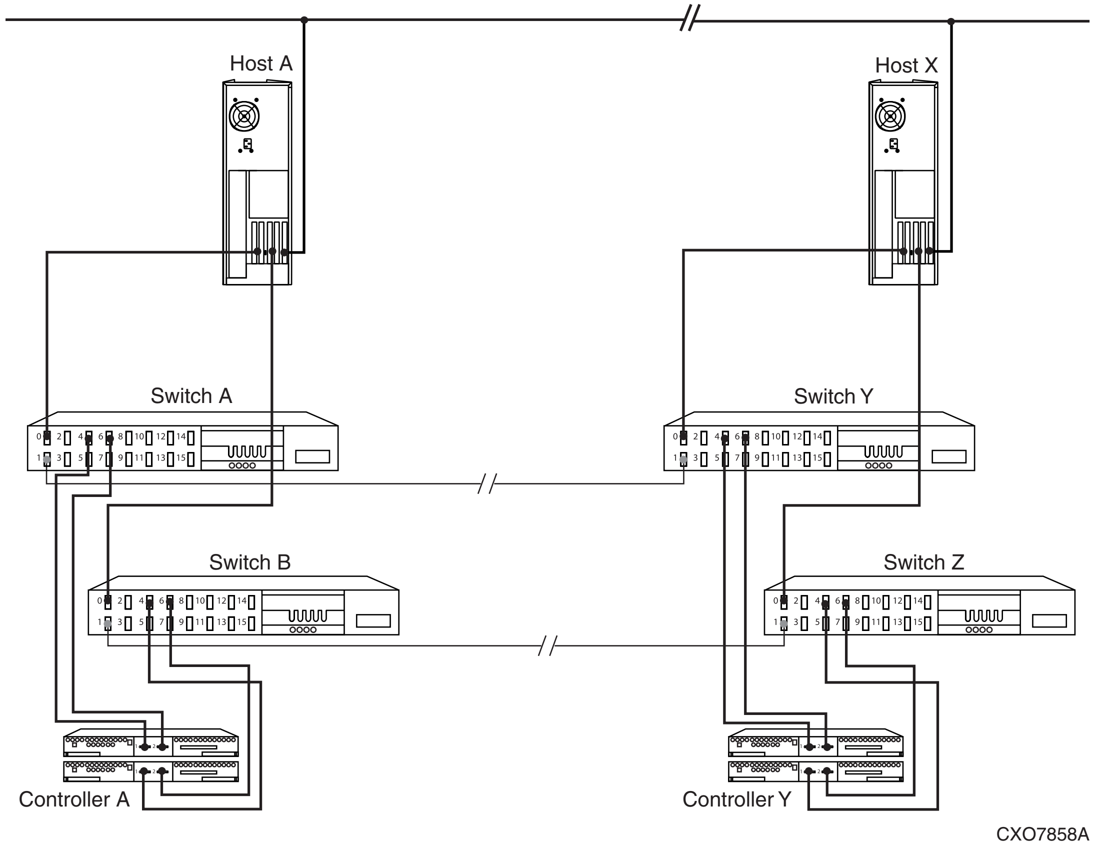

Figure 8: Basic DRM-over-fiber configuration

This dual-fabric SAN provides no single point of failure (NSPOF) at the fabric level. For example, broken cables, switch updates, or an error in switch zoning can cause one fabric to fail, leaving the other to temporarily carry the entire workload. Up to 28 (B-series) switches are supported per fabric. Non-DRM servers and storage are allowed on each fabric as long as each is kept in a zone separate from the DRM solution space. For example, 28 switches may support 96 servers and 8 storage arrays at each site.

As an option, DRM-over-fiber also supports the use of WDM instead of the longwave (10 km) or very long distance (100 km) GBICs. Figure 9 shows a DRM-over-WDM configuration.

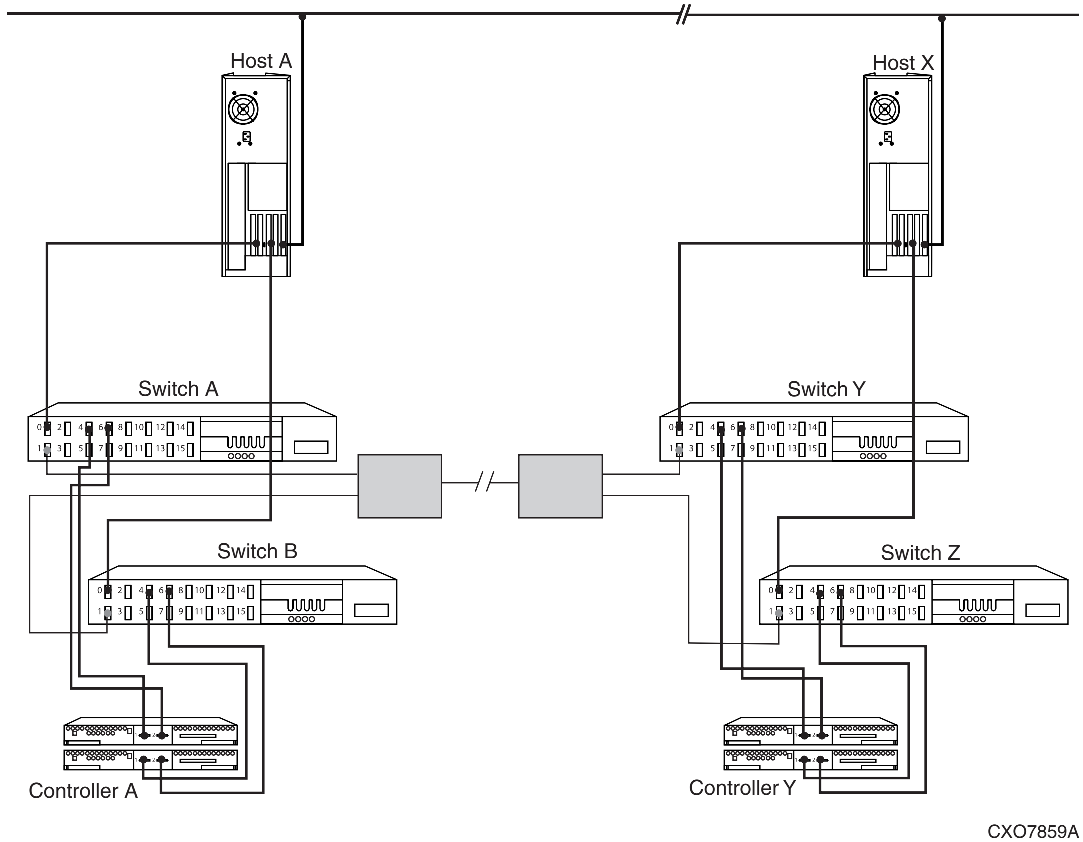

Figure 9: DRM-over-WDM configuration

The difference between the use of WDM and the basic solution is the replacement of at least one, if not both, long-distance GBICs and single-mode fiber with a multiplex unit, shortwave GBICs, and multimode fiber.

DRM engineering has tested equipment from the WDM vendors and concluded that all vendors are supported provided the WDM equipment is configurable to 1- or 2-Gbps speeds, and the switches at either end form part of a fabric. For more information on DRM-over-WDM, refer to the *HP StorageWorks Continuous Access and Data Replication Manager SAN Extensions Reference Guide*.

Basic DRM Configuration Rules

Keep the following requirements in mind when designing your DRM system:

- At least one and no more than eight DRM storage subsystems are required at each initiator (local) site and target (remote) site. Each storage subsystem dedicated to support a DRM configuration must have dual HSG80 controllers and identical drive configurations at both sites.
- Each operating system must either implement multipath support (OpenVMS and Tru64 UNIX) or support it by means of Secure Path software for each pair of HBAs. For Stretched Windows NT/2000 Cluster configurations, the HA/F500 kit includes two copies of Secure Path for Windows NT or Windows 2000.
- Each DRM configuration or instance must be compatible (according to Table 3) with respect to the operating systems sharing the same DRM storage arrays and the configuration's one array.
- The minimum StorageWorks MA8000/EMA12000 configuration supports up to 42 drives per storage array with larger configurations supporting up to 84 drives. Each HSG80 initiator/target controller pair must be of identical geometry, which can consist of JBOD, RAID-0, RAID-1, RAID-0+1, or RAID-3/5 disks. Target LUNs must have the same geometry and must be the same size as the initiator LUNs of the remote copy set.
- Although this document provides configuration rules for the preconfigured MA8000 and EMA12000 storage arrays, the RA8000, ESA12000, and EMA16000 storage arrays are also supported. Initiator and target arrays can be of different architectures (RAID array and modular array) as long as the target storage set has the same geometry and is the same size as the initiator storage set.
- Each HSG80 controller cache module must have 512 MB of memory.
- Each HSG80 controller must have the 8.7P ACS Software Kit installed and running.
- A minimum of two Fibre Channel host bus adapters are required per server to ensure that no single point of failure exists between the server and the storage subsystem.
- Each site must have one DRM documentation set and one storage array platform kit (appropriate for the array type and host operating system) per implemented operating system platform.
- One GBIC that is appropriate for the type of fiber-optic cable being used is required per switch port connection. Appropriate GBIC/fiber-optic cable configurations are:
  - 50-micron multimode fiber (MMF) with 50 micron-compatible shortwave GBICs
  - 9-micron single mode fibre (SMF) with longwave or very long distance GBICs
  - 62.5-micron MMF for attachment to switches with shortwave GBICs when the distance is less than 200 m
  - 8-EL switches with one GBIC for the interswitch link. The other seven ports are preconfigured with shortwave gigabit link modules
  - 16-EL switches with one GBIC per port. Optional power supply not accepted.

A third-party vendor is used to acquire and install all SMF optic cables, any MMF optic cables longer than 50 meters, and WDM interfaces.

As a maximum configuration, DRM-over-fiber (WDM) supports approximately 96 servers and 8 storage arrays per site depending on the SAN topology that is used. A single site with 96 servers and 8 storage arrays using a simple cascaded switch structure is shown in Figure 10.

This structure is not a high-performance SAN because of the use of single switch-to-switch links in order to reduce the switch count. Higher performance SANs can be built using a *skinny tree* topology as defined in the *HP StorageWorks SAN Design Reference Guide*.

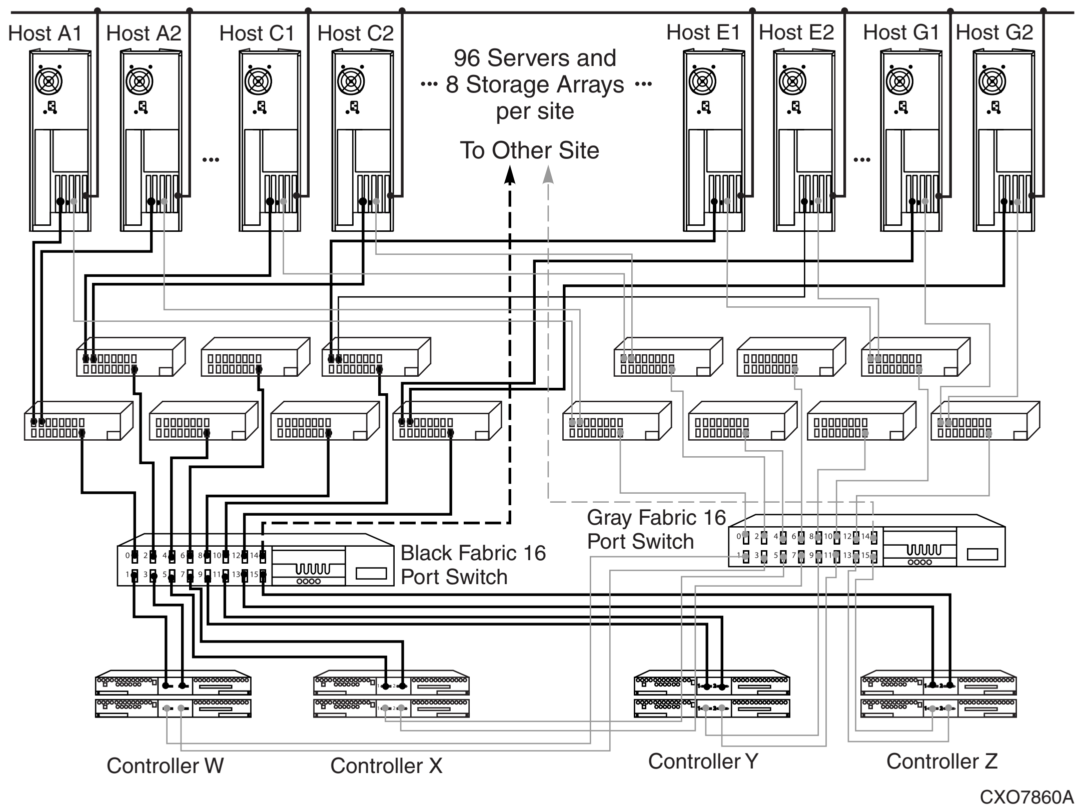

Figure 10: Maximum DRM-over-fiber configuration

Long-Distance Solutions

The following configurations allow the use of DRM over long distances.

Extended DRM-over-ATM configuration

The extended DRM-over-ATM configuration (Figure 11)is similar to the simple DRM configuration except for the use of Fibre Channel-to-ATM gateways from CNT Corporation. Two Fibre Channel-to-ATM gateways are required at each site, one per fabric, for a total of four per solution.

Note: These FC-to-ATM gateways are no longer available for new installations. HP recommends that new installations use an approved FC to IP gateway with an IP router that connects to the ATM backbone.

The size limits listed below only apply if using the CNT Open Systems ATM gateway with version 2.1.9m switch code and Remote Switch Key license. Use the FCIP size limits if using FCIP over ATM.

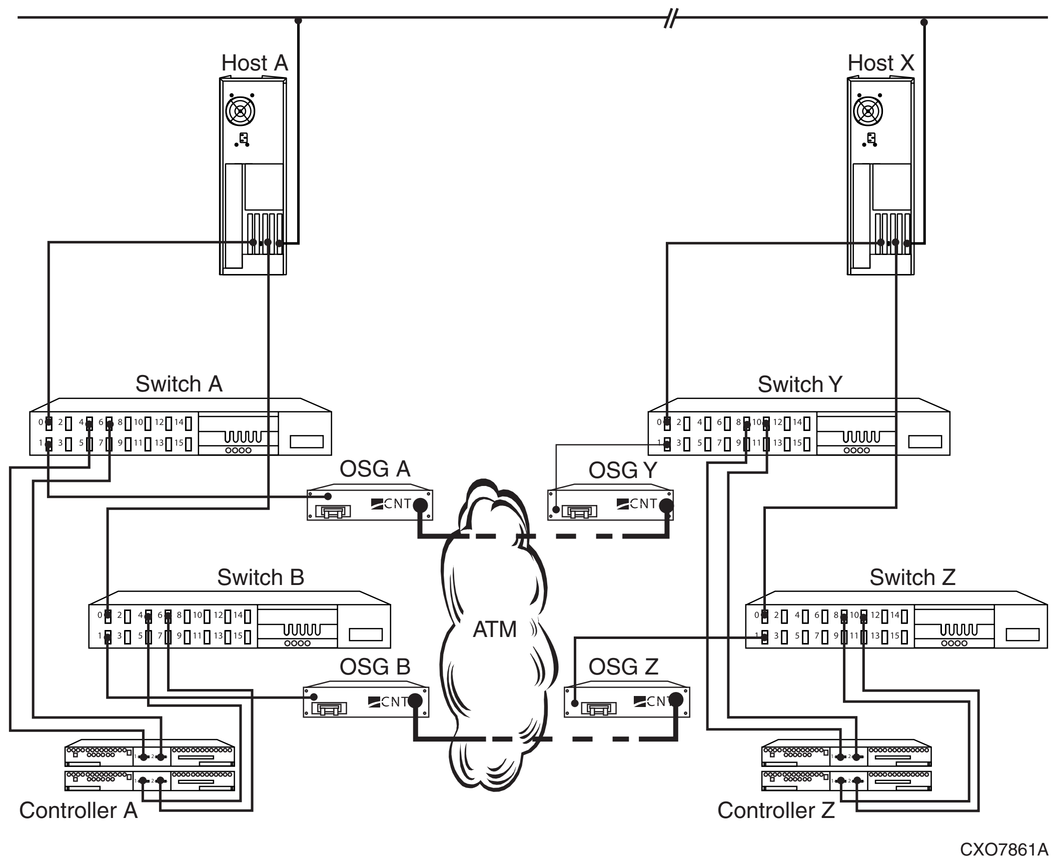

Figure 11: DRM-over-ATM configuration

Because of limitations in the Open System Gateway (OSG), a DRM-over-ATM solution is limited to the available 14 ports on each of the four switches. Support exists for one of the following:

- Up to 12 servers and 1 storage array
- Up to 10 servers and 2 storage arrays
- Up to 8 servers and 3 storage arrays
- Up to 6 servers and 4 storage arrays
- Up to 4 servers and 5 storage arrays
- Up to 2 servers and 6 storage arrays per site

As new implementations of the Fibre Channel-to-ATM gateway functions become available, support for larger DRM-over-ATM solutions should also become available.

Installation of the DRM-over-ATM Remote Switch Key (part number 166601-001) into each of the four switches is required. This key allows either switch to discover what is attached to the other switch at the other end of the ATM link. This key also provides a heartbeat between the two switches to detect loss of the ATM link that may not be reported by the gateways.

DRM-over-ATM and the Fibre Channel-to-ATM gateway support intersite link speeds ranging from 1.54 Mbit/s to 155 Mbit/s. The default connection for the gateway is 155 Mbit/s with MMF. The use of another connection type or speed requires the use of an ATM switch that interfaces with the OC3 multimode output of the gateway into the intersite link. For example, if a pair of classic T1 or E1 intersite links are used, then the ATM switch must support the physical interfaces and data rates of both OC3 and T1 or E1.

DRM-over-ATM also supports the use of external ATM data encryption devices, which allows use of DRM over public ATM networks without concern that the data may be compromised. For more information on the DRM-over-Fibre Channel-to-ATM configuration, refer to the *HP StorageWorks Data Replication Manager over an ATM Link Supporting OSG Version 2.2.5 Application Notes.*

DRM-over-ATM Configuration Rules

Follow these requirements when using ATM:

- At least one and no more than six DRM storage subsystems are required at each initiator (local) site and target (remote) site. Each storage subsystem dedicated to support a DRM configuration must have dual HSG80 controllers and identical drive configurations at both sites.
- Each operating system must either implement multipath support (OpenVMS and Tru64 UNIX) or support it by means of Secure Path software for each pair of HBAs. For Stretched Windows NT and Stretched Windows 2000 Cluster configurations, the HA/F500 kit includes two copies of Secure Path for Windows NT or Windows 2000.
- Each DRM configuration or instance must be compatible (according to Table 3) with respect to the operating systems sharing the same DRM storage arrays and the configuration's one array.
- The minimum StorageWorks MA8000/EMA12000 configuration supports up to 42 drives per storage array with larger configurations supporting up to 84 drives. Each HSG80 initiator/target controller pair must be of identical geometry, which can consist of JBOD, RAID-0, RAID-1, RAID-0+1, or RAID-3/5 disks. Target LUNs must have the same geometry and must be the same size as the initiator LUNs of the remote copy set.
- Although this document provides configuration rules for the preconfigured MA8000 and EMA12000 storage arrays, the RA8000, ESA12000, and EMA16000 storage arrays are also supported. Initiator and target arrays can be of different architectures (RAID array and modular array) as long as the target storage set has the same geometry and is the same size as the initiator storage set.
- Each HSG80 controller cache module must have 512 MB of memory.
- Each HSG80 controller must have the ACS 8.7P Software Kit installed and running.
- A minimum of two Fibre Channel host bus adapters is required per server to ensure that no single point of failure exists between the server and the storage subsystem.
- Each site must have one DRM documentation set and one storage array platform kit appropriate for the array type and host operating system per implemented operating system platform.
- One GBIC that is appropriate for the type of fiber-optic cable being used is required per switch port connection. Appropriate GBIC/fiber-optic cable configurations are:
  - 50-micron MMF with 50 micron-compatible shortwave GBICs
  - 9-micron SMF with longwave or very long distance GBICs.

  - 62.5-micron MMF for attachment to switches with shortwave GBICs when the distance is less than 200 m
  - 8-EL switches with one GBIC for the interswitch link. The other seven ports are preconfigured with shortwave gigabit link module (GLM).
  - 16-EL switches with one GBIC per port. Optional power supply not accepted.
- A third-party vendor is used to acquire and install all SMF optic cables, any MMF optic cables longer than 50 m, and ATM interfaces.
- As a maximum configuration, DRM-over-fiber (ATM) supports up to 1 array and 12 servers, 2 arrays and 10 servers, 3 arrays and 8 servers, 4 arrays and 6 servers, 5 arrays and 4 servers, or 6 arrays and 2 servers per site.
- Each of the four switches in the solution must have the Remote Switch Key (part number 166601-001) installed and running version 2.1.9m switch code.

Extended DRM-over-IP Configuration

The extended DRM-over-IP configuration is similar to the simple DRM configuration except for the use of Fibre Channel-to-IP gateways. Two gateways are required at each site, one per fabric, for a total of four per solution, dedicated to that solution. When multiport gateways become available, each port must be dedicated to another single port. HP also expects to support multisite SANs—for example, where sites A and B are both replicating to storage at site C.

Most Fibre Channel-to-IP gateways do not have the same design limitations as Fibre Channel-to-ATM gateways. The DRM-over-IP solution has the same fabric configuration limitation as DRM-over-fibre solutions, namely 28 (B-series) switches (equivalent to 96 servers and 8 storage arrays).

Initial versions of the Fibre Channel-to-IP gateway support direct connection to either 10/100-Mbit/s or 1-Gbit/s Ethernet. The Fibre Channel-to-IP gateway uses whatever intersite network bandwidth is set aside for the storage interconnect. The IP tunnel that is created to support the Fibre Channel-to-IP traffic also provides enhanced security of the data because of the nature of IP tunnels. HP recommends designing the IP tunnels to carry all the intersite data traffic in case either—but not both—links fail.

For a listing of approved FCIP vendor products for DRM, as well as information on the extended DRM-over-IP configuration, refer to the *HP StorageWorks Continuous Access and Data Replication Manager SAN Extensions Reference Guide*.

Figure 12 shows a DRM-over-IP configuration.

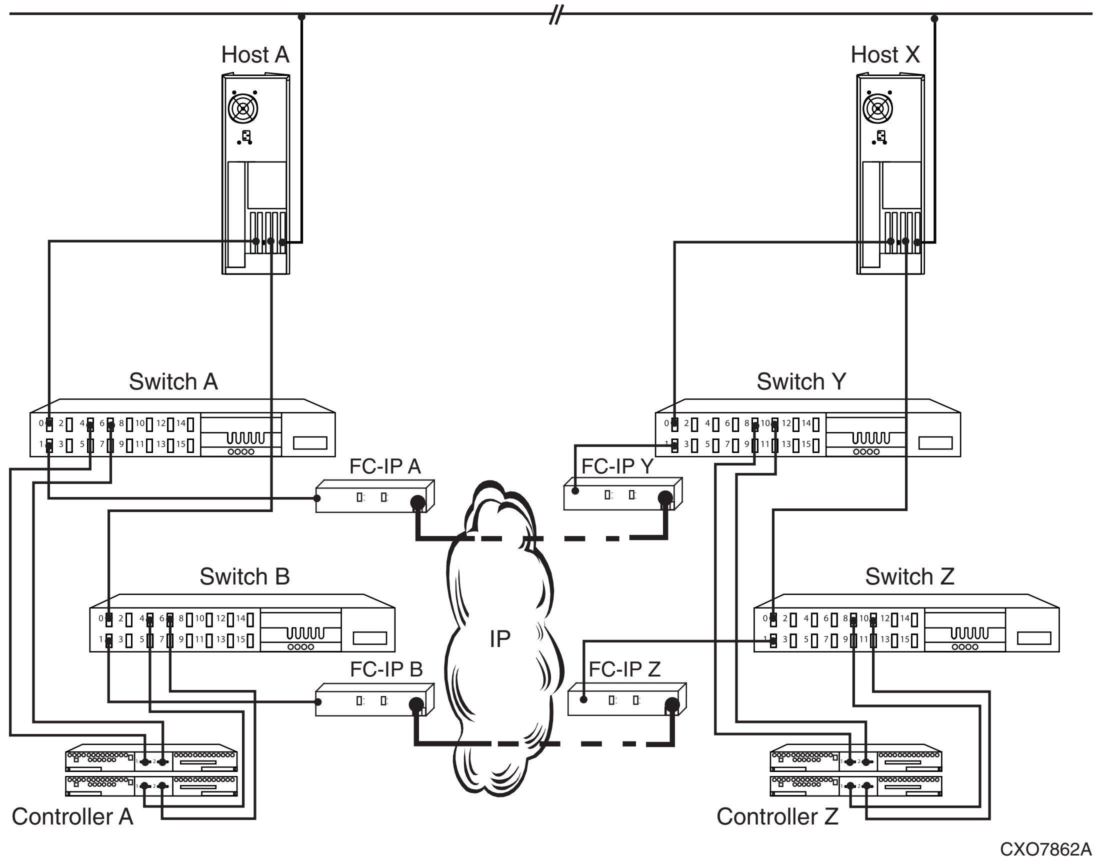

Figure 12: DRM-over-IP configuration

DRM-over-IP Configuration Rules

Observe these requirements when designing a DRM-over-IP system:

- At least one and no more than eight DRM storage subsystems are required at each initiator (local) site and target (remote) site. Each storage subsystem dedicated to support a DRM configuration must have dual HSG80 controllers and identical drive configurations at both sites.
- Each operating system must either implement multipath support (OpenVMS and Tru64 UNIX) or support it by means of Secure Path software for each pair of HBAs.
- Each DRM configuration or instance must be compatible (according to Table 3) with respect to the operating systems sharing the same DRM storage arrays and the configuration's one array.
- The minimum StorageWorks MA8000/EMA12000 configuration supports up to 42 drives per storage array with larger configurations supporting up to 84 drives. Each HSG80 initiator/target controller pair must be of identical geometry, which can consist of JBOD, RAID-0, RAID-1, RAID-0+1, or RAID-3/5 disks. Target LUNs must have the same geometry and must be the same size as the initiator LUNs of the remote copy set.

- Although this document provides configuration rules for the preconfigured MA8000 and EMA12000 storage arrays, the RA8000, ESA12000, and EMA16000 storage arrays are also supported. Initiator and target arrays can be of different architectures (RAID array and modular array) as long as the target storage set has the same geometry and is the same size as the initiator storage set.
- Each HSG80 controller cache module must have 512 MB of memory.
- Each HSG80 controller must have the ACS 8.7P Software Kit installed and running.
- A minimum of two Fibre Channel host bus adapters is required per server to ensure that no single point of failure exists between the server and the storage subsystem.
- Each site must have one DRM documentation set and one storage array platform kit appropriate for the array type and host operating system per implemented operating system platform.
- One GBIC that is appropriate for the type of fiber-optic cable being used is required per switch port connection. Appropriate GBIC/fiber-optic cable configurations are:
  - 50-micron MMF with 50 micron-compatible shortwave GBICs
  - 9-micron SMF with longwave or very long distance GBICs
  - 62.5-micron MMF for attachment to switches with shortwave GBICs when the distance is less than 200 m
  - 8-EL switches with one GBIC for the interswitch link. The other seven ports are preconfigured with shortwave gigabit link module (GLM).
  - 16-EL switches with one GBIC per port. Optional power supply not accepted.

A third-party vendor is used to acquire and install all SMF optic cables, any MMF optic cables longer than 50 meters, and WDM interfaces.

Depending on the vendor, support may be limited to one switch per fabric per site, for a total of four switches in the SAN. Other vendors will support a larger switch configuration.

Testing indicates that some IP gateways provide a mechanism to notify the fabric that connectivity to the remote gateway has been lost. Other gateways require use of a fabric-based heartbeat to detect loss of the intersite IP network connection. Those vendors that require the fabric heartbeat require installation of the remote switch key license onto those two switches that directly connect to the IP gateway. Do not enable suppression of F-Class frames, because doing so will limit the supported size of the DRM-over-IP SAN to one switch at each site.

Refer to the *HP StorageWorks Continuous Access and Data Replication Manager SAN Extensions Reference Guide* for more information on the requirements for remote switch or extended fabric licenses.

Special-Purpose DRM Solutions

The following sections describe different DRM configurations for special circumstances.

Bidirectional DRM Configuration

DRM supports active/active bidirectional solutions by using two sets of storage arrays, one set for each direction. This configuration allows both sites to be actively processing data and backing up each other in the event one of the two sites fails. The HP Storage Solutions team created the bidirectional DRM solution, which is a turnkey deployment of the basic bidirectional DRM for Windows NT® and Windows 2000. For more information on this solution, go to

http://h18000.www1.hp.com/products/storageworks/solutions/bidirectdrm/index.html.

As shown in Figure 13, there are two servers at each site. These site-specific pairs of servers can be clustered during normal operations to provide highly available applications. When a failure occurs at one of the sites, the application that was running at the failed site is moved to the backup member of the surviving cluster and started using the surviving storage and the other half of the surviving cluster.

With additional servers and storage, the bidirectional DRM can scale to 28 (B-series) switches in each fabric, supporting up to 96 servers and 8 arrays at each site. All intersite technologies, such as DRM-over-ATM, direct fiber, IP, and WDM, support bidirectional use of DRM.

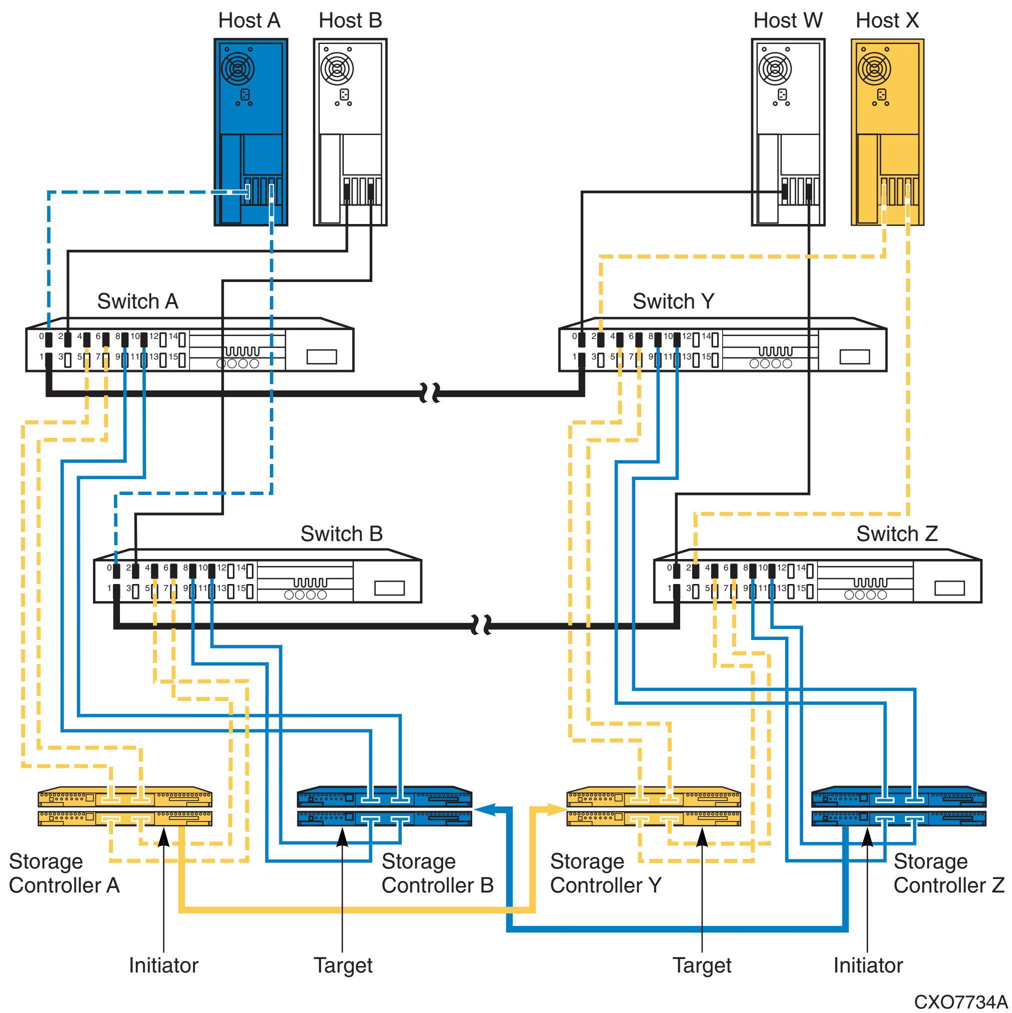

Figure 13: Bidirectional DRM configuration

Stretched Cluster Support

DRM supports stretched Microsoft Cluster Servers (MSCS) running Windows 2000 or Windows NT. In this configuration, shown in Figure 14, half the cluster is at the primary site and the other half is at the alternate site. If the primary server fails, MSCS fails over the application to the surviving server at the alternate site and resumes operations using the primary site storage.

Applications running in a stretched cluster in failover mode incur a performance penalty because of the time it takes to read or write data across the intersite link. This performance penalty is directly proportional to the distance between the two sites. During testing, almost no additional impact was observed with separation distances up to 100 km. For more information on stretched cluster support, see the HP ProLiant HA/F500 website at:

http://h18000.www1.hp.com/solutions/enterprise/highavailability/microsoft/haf500/description-dt.html

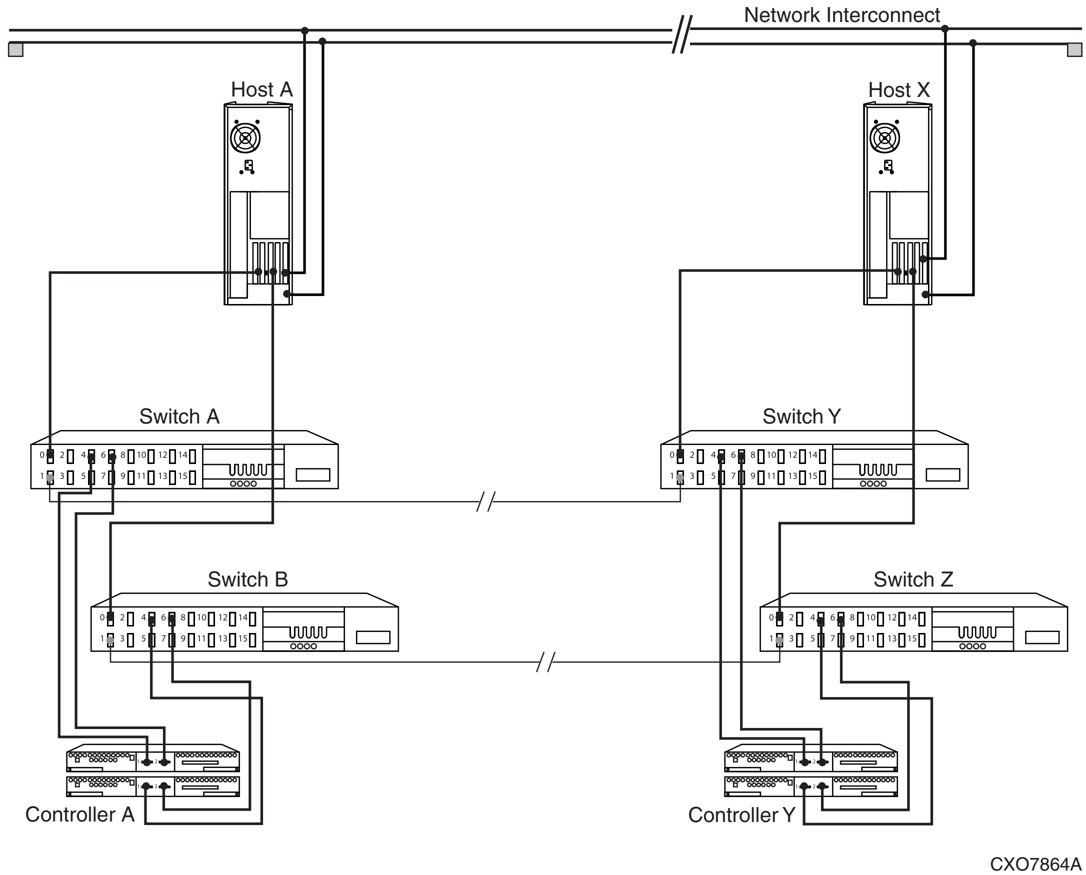

Figure 14: DRM stretched cluster

In addition to Windows 2000 and Windows NT stretched cluster support, HP also supports HP Tru64 UNIX Campus-Wide Disaster Tolerant Cluster—Alpha servers running Tru64 UNIX TruClusters coupled with DRM. This configuration allows a standard Tru64 UNIX TruCluster implementation to stretch geographically to a maximum of 6 km.

This stretch cluster option allows you to design fully scalable high-availability configurations comprising from two to eight AlphaServer systems distributed between two sites, and from one to four mirrored HP StorageWorks storage subsystems per site. Spans may be up to 2 km without Memory Channel (MC) hubs, up to 3 km with redundant local MC hubs (one hub at each site), and up to 6 km with the use of redundant MC hubs located midway between sites. Also supported is synchronous replication of cluster (except quorum) data file systems from the initiator site to the target site.

HP Tru64 UNIX Campus-Wide Disaster Tolerant Cluster includes detailed documentation on disaster tolerant actions and procedures such as a site failover and failback. For additional information, visit the HP website at:

http://h30097.www3.hp.com/cluster/tru64_campus_clusters.html

DRM Dual-Switch/Single-Site Configuration

HP supports the DRM dual switch/single site configuration for those environments that need only local data protection in the event of local disasters, or that are used as local test beds for operational DRM solutions. This solution uses only two switches, where each switch creates a fabric "in a box" instead of the multiswitch fabrics supported in the non-dual-switch/single-site DRM solutions.

Because of its design, a DRM dual-switch/single-site configuration is limited to supporting the connections available on one switch (8 to 64 ports). Therefore, given a DRM dual-switch/single-site configuration consisting of two 16-port switches, the maximum configuration can be one of the following:

- 1 pair of arrays and 12 servers
- 2 pairs of arrays and 8 servers
- 3 pairs of arrays and 4 servers

Both the HSG80 and the server HBA use only shortwave GBICs. Therefore, the DRM dual-switch/single-site configuration is limited to 500 meters of 50-micron or 200 meters of 62.5-micron multimode fiber-optic cable between the HBA and either switch, and another 500 meters of 50-micron or 200 meters of 62.5-micron multimode fiber-optic cable from the controller to either switch. This configuration limits the DRM dual-switch/single-site configuration to a maximum separation of 1 km using 50-micron cable (400 meters with 62.5-micron cable) between primary and alternate sites.

To achieve this maximum distance, HP recommends locating the two switches somewhere between the primary site and the alternate site. Install the switches in separate locations with unique fiber paths between the switch and both sites, as shown in Figure 15.

The DRM dual-switch/single-site configuration is not designed to survive even local natural disasters, such as tornadoes, earthquakes, or hurricanes, because of the limited intersite distance. This configuration also may not survive or continue to operate after two unrelated failures, due to its limited NSPOF configuration.

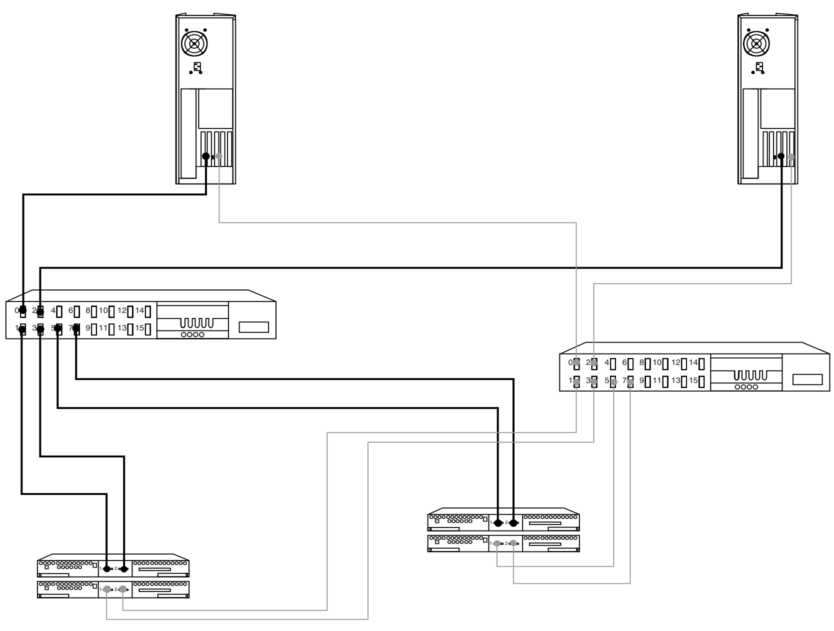

Figure 15: DRM dual-switch/single-site configuration

Single-Fabric Configuration

The single fabric DRM solution is designed for small, entry-level tests or proof-of-concept demonstrations where some distance is needed between each of the two switches in the solution. This solution can also be used for producing copies of data needed for data migration or data mining.

Fabric zoning is used to create two logical fabrics out of the one physical fabric. At this writing, the maximum configuration is two 64-port switches—one per site. Using 16-port switches, these two switches share one intersite link, leaving up to 15 ports for servers and storage controllers. Those 15 ports support up to:

- Five servers and one array
- Three servers and two arrays, or
- One server and three arrays per site.

An example of the single fabric configuration is shown in Figure 16.

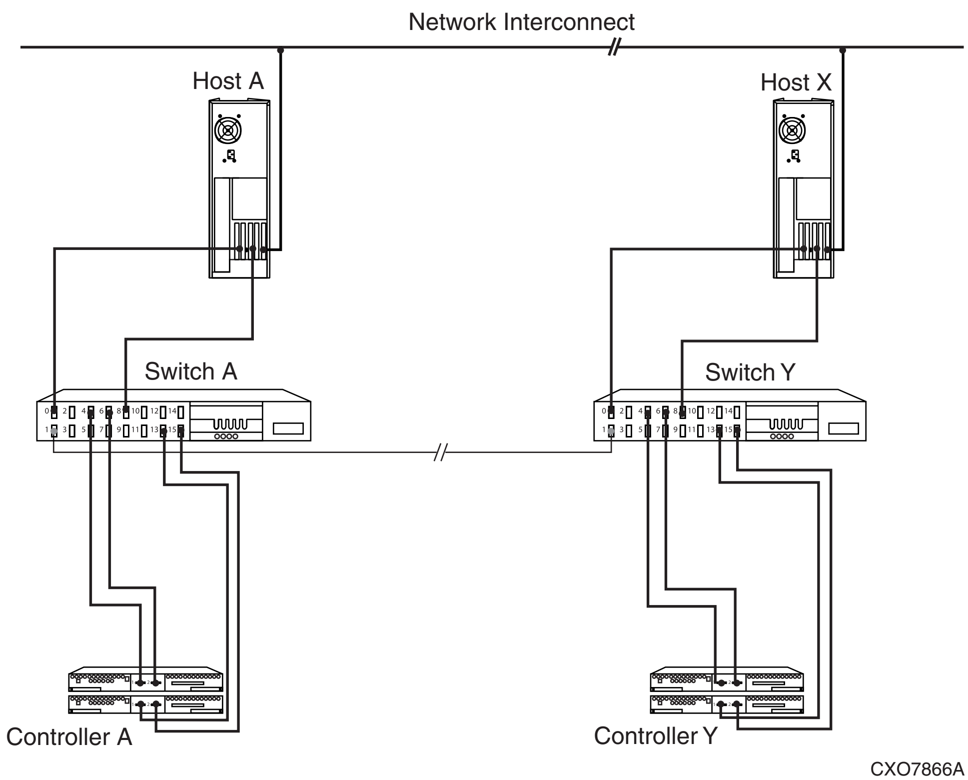

Figure 16: Single-fabric configuration

Single-Switch Configuration

The single-switch DRM solution is designed for small, single-site, entry-level tests or proof-of-concept demonstrations. This non-disaster-tolerant solution can also be used for producing copies of data needed for data migration or data mining. At this writing, the maximum configuration is one 64-port switch, where four ports are used for each fabric at each site. These four ports can support a maximum of two servers and one storage array per simulated site. Fabric zoning is used to create the two logical fabrics used by DRM. An example of the single-switch solution is shown in Figure 17.

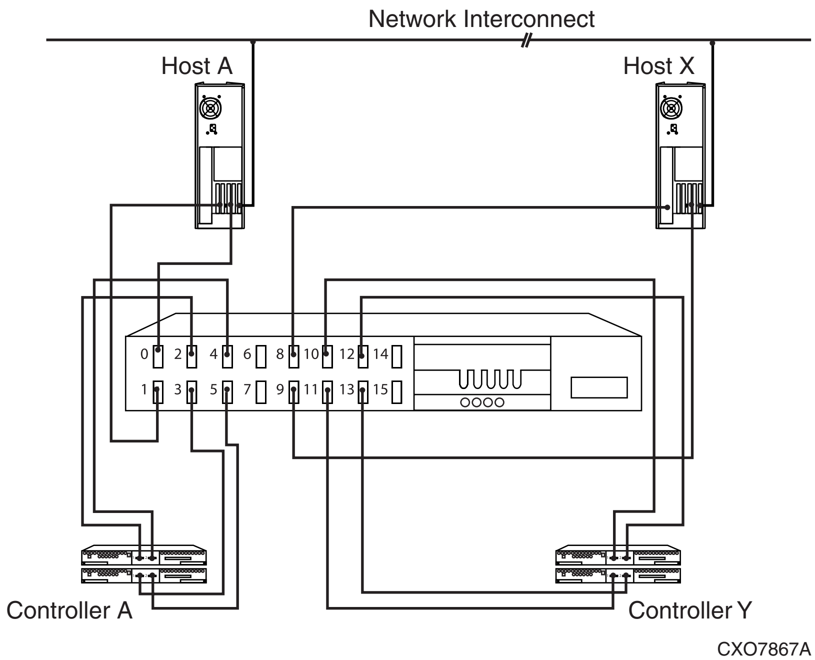

Figure 17: Single-switch configuration

Supportable Solution Checklists

A

This appendix provides tables to use as a checklist to make sure that you have ordered the required software and hardware for your DRM solution.

Note: The part numbers provided below are for reference only. Some items are no longer manufactured, are obsolete, or cannot be purchased. They are provided to help you refer to items that were part of a solution at one time.

The following configurations are listed:

Basic DRM or DRM-over-WDM Configurations

Table 10 through Table 18 contain a partial parts list for basic DRM or DRM-over-WDM configurations.

Table 10: MA/EMA Storage Cabinet

Description	Maximum Number of Drives	60 Hz Part Number	50 Hz Part Number
MA 8000: 1 M2200, 3 4254, 22U Opal Cab	42 per cabinet	175992-B21	175992-B22
EMA 12000 D14: 3 M2200, 9 4254, 42U Opal Cab	42 per M2200	175990-B21	175990-B22
EMA 12000 S14: 1 M2200, 6 4214, 42U Opal Cab	84 per cabinet	175991-B21	175991-B22
EMA 12000 BLUE: 1 M2200, 3 4254, 41U Blue Cab	42 per cabinet	175993-B21	175993-B22
EMA 16000 D14: 2 M2200, 12 4354R, 42U Opal Cab	84 per M2200	238792-B21	238792-B22
EMA 16000 S14: 1 M2200, 12 4314R, 42U Opal Cab	168 per cabinet	238791-B21	238791-B22

Quantities are based on number of required drives and number of drives per SCSI bus.

Table 11: Required Controller and Cache Upgrades

Description	Quantity Required	Part Number
HSG80 with 256-MB Cache	4 (2 per site)	176622-B21
M2200 External Cache Battery	4 (2 per site)	135823-B21
256 MB Cache Upgrade	4 (2 per site)	380674-B21
HSG80 Controller Software-ACS 8.7P	4 (2 per site)	222316-B23
ACS 8.xG Upgrade to ACS 8.7P	4 (2 per site)	222370-B23
ACS 8.xL Upgrade to ACS 8.7P	4 (2 per site)	222369-B23
ACS 8.xF Upgrade to ACS 8.7P	4 (2 per site)	222371-B23
ACS 8.xS Upgrade to ACS 8.7P	4 (2 per site)	222372-B23
ACS 8.xP Upgrade to ACS 8.7P	4 (2 per site)	222317-B23

Table 12: Required Host Software

Description	Quantity Required	Part Number
HSG80 Solution Software for HP-UX	One copy per site	279823-B21
HSG80 Solution Software for IBM-AIX	One copy per site	279827-B21
HSG80 Solution Software for Novell NetWare	One copy per site	279815-B21
HSG80 Solution Software for OpenVMS	One copy per site	279807-B21
HSG80 Solution Software for Sun Solaris	One copy per site	279819-B21
HSG80 Solution Software for Tru64 UNIX	One copy per site	279803-B21
HSG80 Solution Software for Windows NT/2000	One copy per site	279811-B21

Table 13: Additional Required Software for HP, Novell, Sun, or Windows

Description	Quantity Required	Part Number
HP, Secure Path Host 3.0	2 (1 per site)	261705-B21
IBM, Secure Path Host 2.0A	2 (1 per site)	231495-B21
Novell, Secure Path Host 3.0B	2 (1 per site)	165993-B21
Sun, Secure Path Host 3.0A	2 (1 per site)	165991-B22
Windows Secure Path Host 3.1A	2 (1 per site)	213076-B22
Windows Secure Path Host 4.0	2 (1 per site)	165989-B22
Windows, HA/F500 Enhanced DT Cluster	1	164227-B21

Table 14: Disk Drives

Description	Part Number
72-GB Ultra 3 SCSI, 10,000-rpm, 1.6-inch drive	176494-B21
72-GB Ultra 3 SCSI, 10,000-rpm, 1-inch drive	232432-B22
36-GB Ultra 3 SCSI, 10,000-rpm, 1-inch drive	176496-B22
36-GB Ultra 3 SCSI, 15,000-rpm, 1-inch drive	232916-B22
18-GB Ultra 3 SCSI, 15,000-rpm, 1-inch drive	188122-B22
9-GB Ultra 3 SCSI, 15,000-rpm, 1-inch drive	188120-B22
18-GB Ultra 3 SCSI, 10,000-rpm, 1-inch drive	142673-B22
9-GB Ultra 3 SCSI, 10,000-rpm, 1-inch drive	142671-B22
18-GB Ultra 2 SCSI, 10,000-rpm, 1-inch drive	128418-B22
9-GB Ultra 2 SCSI, 10,000-rpm, 1-inch drive	328939-B22
18-GB Ultra 2 SCSI, 7,200-rpm, 1-inch drive	388411-B22
9-GB Ultra 2 SCSI, 7,200-rpm, 1-inch drive	123065-B22

Order in pairs and ship half per site so that the total drives do not exceed the drive quantities in Table 10.

Table 15: Host Bus Adapters

Description	Quantity Required	Part Number
Note: In addition to the host bus adapters listed below, refer to the DRM Release Notes for more approved host bus adapters. Order these in pairs for each supported server.		
Alpha/Tru64 UNIX or OpenVMS KGPSA-CA	4 (2 per site)	168794-B21
HP-UX PCI HBA (1Gb)	4 (2 per site)	A5158A
HP-UX PCI HBA (2Gb)	4 (2 per site)	A6795A
IBM AIX	4 (2 per site)	197819-B21
Novell 64-bit/66-MHz HBA	4 (2 per site)	120186-B21
Sun 32-bit PCI HBA	4 (2 per site)	254456-B21
Sun cPCI HBA (Sun Solaris V8 only)	2 (2 per site)	254457-B21
Sun 64-bit SBus HBA	4 (2 per site)	254458-B21
Windows 2000 or Windows NT KGPSA-CB	4 (2 per site)	176479-B21

Table 16: Fibre Channel Switches

Description	Quantity Required	Part Number
Note: Refer to the DRM Release Notes for additional Fibre Channel switches that are supported. In addition to the B- and M-series switches listed below, C-series switches have been approved for use with DRM.		
B-series switches		
Fibre Channel SAN Switch, 16-port	4 (2 per site)	158223-B21
Fibre Channel SAN Switch, 8-port	4 (2 per site)	158222-B21
Fibre Channel SAN Switch, 8-EL	4 (2 per site)	176219-B21
Fibre Channel SAN Switch, 16-EL	4 (2 per site)	212776-B21
SAN Switch 2/16, 16-port, 2 Gb	4 (2 per site)	287055-B21
SAN Switch 2/16-EL, 16-port, 2 Gb	4 (2 per site)	283056-B21
SAN Switch 2/8, 8-port, 2 Gb	4 (2 per site)	258707-B21
StorageWorks Core Switch 2/64, 64-port, 2 Gb	2 (1 per site)	254508-B21
Optional Switch Rack-Mount Kit	4 (2 per site)	167365-B21
Optional Redundant Switch Power Supply (for 8- and 16-port Fibre Channel Switch)	4 (2 per site)	160407-B21
Extended Fabric License	1 per site	262868-B21
M-series switches		
StorageWorks SAN Director 64, 1 Gb	2 (1 per site)	254512-B21
StorageWorks Director 2/64, 64-port, 2 Gb	2 (1 per site)	286809-B21
StorageWorks Edge 2/32, 32-port, 2 Gb	4 (2 per site)	286810-B21
StorageWorks Edge 2/16, 16-port, 2 Gb	4 (2 per site)	286811-B21
Fibre Channel Switch, ES-3032	4 (2 per site)	order from vendor

Table 17: Fibre Channel Cables and GBICs MMF Cables

Description	Quantity Required	Part Number
Fibre Channel short-distance GBIC	Minimum of 12 (half per site)	380561-B21
Fibre Channel cable kit (2 GBICs, two 2-m cables)	Minimum of 6 pairs	380596-B21
Fibre Channel cable, multimode (2 m)	Minimum of 6 pairs	234457-B21
Fibre Channel cable, multimode (5 m)	Minimum of 6 pairs	234457-B22
Fibre Channel cable, multimode (15 m)	Minimum of 6 pairs	234457-B23
Fibre Channel cable, multimode (30 m)	Minimum of 6 pairs	234457-B24
Fibre Channel cable, multimode (50 m)	Minimum of 6 pairs	234457-B25

Order a minimum of 6 pairs of MMF cables and 12 GBICs and ship half per site.

Table 18: Other Required Items for Long Distance Direct Fiber Connections

Description	Quantity Required	Part Number
10-km long distance GBIC	4 (2 per site)	127508-B21
100-km very long distance GBIC	4 (2 per site)	230800-B21

Order MMF cables and GBICs to connect a WDM multiplexer to switch.

Additional considerations (order items from third-party vendors):

- Each WDM channel supports full bandwidth Fibre Channel connections up to 1 Gb/s when using WDM.
- For SMF optic cable, order 2 intersite cables.
- Longwave SMF cable up to 100 km. The cable must be duplex tight buffered SMF 9/125 um (Belcore GR-409 or ITU G.652) compliant. The connectors must be SC duplex low metal (NTT-SC Belcore 326 or IEC-874-19 SC) compliant.
- Seven of 8 ports on 8-EL switches and all ports on the HSG80 and HBA come with integrated SR GBICs. Therefore, each EL switch needs 1 SR, LD, VLD GBIC per interswitch link.
- WDM uses the same 9-micron cable for the intersite link. WDM may be used for multiple site-to-site links, such as the network, in addition to Fibre Channel connections.

DRM Fibre Channel-over-ATM Configurations

Table 19 through Table 26 contain a partial parts list for DRM-over-ATM configurations.

Table 19: MA/EMA Storage Cabinet

Description	Maximum Number of Drives	60 Hz Part Number	50 Hz Part Number
MA 8000: 1 M2200, 3 4254, 22U Opal Cab	42 per cabinet	175992-B21	175992-B22
EMA 12000 D14: 3 M2200, 9 4254, 42U Opal Cab	42 per M2200	175990-B21	175990-B22
EMA 12000 S14: 1 M2200, 6 4214, 42U Opal Cab	84 per cabinet	175991-B21	175991-B22
EMA 12000 BLUE: 1 M2200, 3 4254, 41U Blue Cab	42 per cabinet	175993-B21	175993-B22
EMA 16000 D14: 2 M2200, 12 4354R, 42U Opal Cab	84 per M2200	238792-B21	238792-B22
EMA 16000 S14: 1 M2200, 12 4314R, 42U Opal Cab	168 per cabinet	238791-B21	238791-B22

These quantities are based on number of required drives and number of drives per SCSI bus—order two, ship one per site.

Table 20: Required Controller and Cache Upgrades

Description	Quantity Required	Part Number
HSG80 with 256-MB Cache	4 (2 per site)	176622-B21
M2200 External Cache Battery	4 (2 per site)	135823-B21
256 MB Cache Upgrade	4 (2 per site)	380674-B21
HSG80 Controller Software-ACS 8.7P	4 (2 per site)	222316-B23
ACS 8.xG Upgrade to ACS 8.7P	4 (2 per site)	222370-B23
ACS 8.xL Upgrade to ACS 8.7P	4 (2 per site)	222369-B23
ACS 8.xF Upgrade to ACS 8.7P	4 (2 per site)	222371-B23
ACS 8.xS Upgrade to ACS 8.7P	4 (2 per site)	222372-B23
ACS 8.xP Upgrade to ACS 8.7P	4 (2 per site)	222317-B23

Table 21: Required Host Software

Description	Quantity Required	Part Number
HSG80 Solution Software for HP-UX	One copy per site	279823-B21
HSG80 Solution Software for IBM-AIX	One copy per site	279827-B21
HSG80 Solution Software for Novell NetWare	One copy per site	279815-B21
HSG80 Solution Software for OpenVMS	One copy per site	279807-B21
HSG80 Solution Software for Sun Solaris	One copy per site	279819-B21
HSG80 Solution Software for Tru64 UNIX	One copy per site	279803-B21
HSG80 Solution Software for Windows NT/2000	One copy per site	279811-B21

Table 22: Additional Required Software for HP, Novell, Sun, or Windows

Description	Quantity Required	Part Number
Note: Refer to the DRM Release Notes for the current versions of HP StorageWorks Secure Path applications.		
HP-UX Secure Path Host	2 (1 per site)	261705-B21
IBM-AIX Secure Path Host	2 (1 per site)	231495-B21
Novell Netware Secure Path Host	2 (1 per site)	165993-B21
MS Windows Secure Path Host 3.x	2 (1 per site)	213076-B22
MS Windows Secure Path Host 4.x	2 (1 per site)	165989-B22
MS Windows, HA/F500 Enhanced DT Cluster	1	164227-B21
Sun Solaris Secure Path Host	2 (1 per site)	165991-B22

Table 23: Disk Drives

Description	Part Number
72-GB Ultra 3 SCSI, 10,000-rpm, 1.6-inch drive	176494-B21
72-GB Ultra 3 SCSI, 10,000-rpm, 1-inch drive	232432-B22
36-GB Ultra 3 SCSI, 10,000-rpm, 1-inch drive	176496-B22
36-GB Ultra 3 SCSI, 15,000-rpm, 1-inch drive	232916-B22
18-GB Ultra 3 SCSI, 15,000-rpm, 1-inch drive	188122-B22
9-GB Ultra 3 SCSI, 15,000-rpm, 1-inch drive	188120-B22
18-GB Ultra 3 SCSI, 10,000-rpm, 1-inch drive	142673-B22
9-GB Ultra 3 SCSI, 10,000-rpm, 1-inch drive	142671-B22
18-GB Ultra 2 SCSI, 10,000-rpm, 1-inch drive	128418-B22
9-GB Ultra 2 SCSI, 10,000-rpm, 1-inch drive	328939-B22
18-GB Ultra 2 SCSI, 7,200-rpm, 1-inch drive	388411-B22
9-GB Ultra 2 SCSI, 7,200-rpm, 1-inch drive	123065-B22

Order in pairs and ship half per site so that the total drives do not exceed the drive quantities in Table 19

.

Table 24: Host Bus Adapters

Description	Quantity Needed	Part Number
Note: In addition to the host bus adapters listed below, refer to the DRM Release Notes for more approved host bus adapters. Order these in pairs for each supported server.		
Alpha/Tru64 UNIX or OpenVMS KGPSA-CA	4 (2 per site)	168794-B21
HP-UX PCI HBA (1Gb)	4 (2 per site)	A5158A
HP-UX PCI HBA (2Gb)	4 (2 per site)	A6795A
IBM AIX	4 (2 per site)	197819-B21
Novell 64-bit/66-MHz HBA	4 (2 per site)	120186-B21
Sun 32-bit PCI HBA	4 (2 per site)	254456-B21
Sun cPCI HBA (Sun Solaris V8 only)	2 (2 per site)	254457-B21
Sun 64-bit SBus HBA	4 (2 per site)	254458-B21
Windows 2000 or Windows NT KGPSA-CB	4 (2 per site)	176479-B21

Table 25: Other Required Items (select one)

Description	Quantity Needed	Part Number
Note: This table remains unchanged due to limits of the CNT Fibre Channel to ATM gateway.		
Fibre Channel Switch, 16 port	4 (2 per site)	158223-B21
Fibre Channel SAN Switch, 8-port	4 (2 per site)	158222-B21
Fibre Channel SAN Switch, 8-EL	4 (2 per site)	176219-B21
Fibre Channel SAN Switch, 16-EL	4 (2 per site)	212776-B21
SAN Switch 2/16, 16-port, 2 Gb	4 (2 per site)	287055-B21
SAN Switch 2/16-EL, 16-port, 2 Gb	4 (2 per site)	283056-B21
SAN Switch 2/8, 8-port, 2 Gb	4 (2 per site)	258707-B21
StorageWorks Core Switch 2/64, 64-port, 2 Gb	2 (1 per site)	254508-B21
Optional Switch Rack-Mount Kit	4 (2 per site)	167365-B21
Optional Redundant Switch Power Supply (for 8- and 16-port Fibre Channel Switch)	4 (2 per site)	160407-B21
Extended Fabric License	1 per site	262868-B21
StorageWorks SAN Director 64, 1 Gb	2 (1 per site)	254512-B21
StorageWorks Director 2/64, 64-port, 2 Gb	2 (1 per site)	286809-B21
StorageWorks Edge 2/32, 32-port, 2 Gb	4 (2 per site)	286810-B21
StorageWorks Edge 2/16, 16-port, 2 Gb	4 (2 per site)	286811-B21
Fibre Channel Switch, ES-3032	4 (2 per site)	order from vendor

Table 26: Fibre Channel Cables and GBICs MMF Cables

Description	Quantity Needed	Part Number
Fibre Channel Short Distance GBIC	Minimum of 12 (half per site)	380561-B21
Fibre Channel Cable Kit (2 GBICs, two 2-m cables)	Minimum of 6 pairs	380596-B21
Fibre Channel Cable Multimode (2m)	Minimum of 6 pairs	234457-B21
Fibre Channel Cable Multimode (5m)	Minimum of 6 pairs	234457-B22
Fibre Channel Cable Multimode (15m)	Minimum of 6 pairs	234457-B23
Fibre Channel Cable Multimode (30m)	Minimum of 6 pairs	234457-B24
Fibre Channel Cable Multimode (50m)	Minimum of 6 pairs	234457-B25

Order a minimum of 6 pairs of MMF cables and 12 GBICs and ship half per site.

DRM Fiber Channel-over-IP Configurations

Table 27 through Table 34 contain a partial parts list for DRM-over-IP configurations.

Table 27: MA/EMA Storage Cabinets

Description	Maximum Number of Drives	60 Hz Part Number	50 Hz Part Number
MA 8000: 1 M2200, 3 4254, 22U Opal Cab	42 per cabinet	175992-B21	175992-B22
EMA 12000 D14: 3 M2200, 9 4254, 42U Opal Cab	42 per M2200	175990-B21	175990-B22
EMA 12000 S14: 1 M2200, 6 4214, 42U Opal Cab	84 per cabinet	175991-B21	175991-B22
EMA 12000 BLUE: 1 M2200, 3 4254, 41U Blue Cab	42 per cabinet	175993-B21	175993-B22
EMA 16000 D14: 2 M2200, 12 4354R, 42U Opal Cab	84 per M2200	238792-B21	238792-B22
EMA 16000 S14: 1 M2200, 12 4314R, 42U Opal Cab	168 per cabinet	238791-B21	238791-B22

Quantities are based on number of required drives and number of drives per SCSI bus. Order two, ship one per site.

Table 28: Required Controller and Cache Upgrades

Description	Quantity Needed	Part Number
HSG80 with 256-MB Cache	4 (2 per site)	176622-B21
M2200 External Cache Battery	4 (2 per site)	135823-B21
256 MB Cache Upgrade	4 (2 per site)	380674-B21
HSG80 Controller Software-ACS 8.7P	4 (2 per site)	222316-B23
ACS 8.xG Upgrade to ACS 8.7P	4 (2 per site)	222370-B23
ACS 8.xL Upgrade to ACS 8.7P	4 (2 per site)	222369-B23
ACS 8.xF Upgrade to ACS 8.7P	4 (2 per site)	222371-B23
ACS 8.xS Upgrade to ACS 8.7P	4 (2 per site)	222372-B23
ACS 8.xP Upgrade to ACS 8.7P	4 (2 per site)	222317-B23

Table 29: Required Host Software

Description	Quantity Needed	Part Number
HSG80 Solution Software for HP-UX	One copy per site	279823-B21
HSG80 Solution Software for IBM-AIX	One copy per site	279827-B21
HSG80 Solution Software for Novell NetWare	One copy per site	279815-B21
HSG80 Solution Software for OpenVMS	One copy per site	279807-B21
HSG80 Solution Software for Sun Solaris	One copy per site	279819-B21
HSG80 Solution Software for Tru64 UNIX	One copy per site	279803-B21
HSG80 Solution Software for Windows NT/2000	One copy per site	279811-B21

Table 30: Additional Required Software for HP, Novell, Sun, or Windows

Description	Quantity Needed	Part Number
Note: Refer to the DRM Release Notes for the current versions of HP StorageWorks Secure Path applications.		
HP-UX Secure Path Host	2 (1 per site)	261705-B21
IBM AIX Secure Path Host	2 (1 per site)	231495-B21
Novell Netware Secure Path Host	2 (1 per site)	165993-B21
MS Windows Secure Path Host 3.x	2 (1 per site)	213076-B22
MS Windows Secure Path Host 4.x	2 (1 per site)	165989-B22
MS Windows, HA/F500 Enhanced DT Cluster	1	164227-B21
Sun Solaris Secure Path Host	2 (1 per site)	165991-B22

Table 31: Disk Drives

Description	Part Number
72-GB Ultra 3 SCSI, 10,000-rpm, 1.6-inch drive	176494-B21
72-GB Ultra 3 SCSI, 10,000-rpm, 1-inch drive	232432-B22
36-GB Ultra 3 SCSI, 10,000-rpm, 1-inch drive	176496-B22
36-GB Ultra 3 SCSI, 15,000-rpm, 1-inch drive	232916-B22
18-GB Ultra 3 SCSI, 15,000-rpm, 1-inch drive	188122-B22
9-GB Ultra 3 SCSI, 15,000-rpm, 1-inch drive	188120-B22
18-GB Ultra 3 SCSI, 10,000-rpm, 1-inch drive	142673-B22
9-GB Ultra 3 SCSI, 10,000-rpm, 1-inch drive	142671-B22
18-GB Ultra 2 SCSI, 10,000-rpm, 1-inch drive	128418-B22
9-GB Ultra 2 SCSI, 10,000-rpm, 1-inch drive	328939-B22
18-GB Ultra 2 SCSI, 7,200-rpm, 1-inch drive	388411-B22
9-GB Ultra 2 SCSI, 7,200-rpm, 1-inch drive	123065-B22
9 GB Ultra 2 SCSI, 7,200-rpm, 1-inch drive	123065-B22

Order in pairs and ship half per site so that the total drives do not exceed the drive quantities in Table 27.

Table 32: Host Bus Adapters

Description	Quantity Required	Part Number
Note: In addition to the host bus adapters listed below, refer to the DRM Release Notes for more approved host bus adapters. Order these in pairs for each supported server.		
Alpha/Tru64 UNIX or OpenVMS KGPSA-CA	4 (2 per site)	168794-B21
HP-UX PCI HBA (1Gb)	4 (2 per site)	A5158A
HP-UX PCI HBA (2Gb)	4 (2 per site)	A6795A
IBM AIX	4 (2 per site)	197819-B21
Novell 64-bit/66-MHz HBA	4 (2 per site)	120186-B21
Sun 32-bit PCI HBA	4 (2 per site)	254456-B21
Sun cPCI HBA (Sun Solaris V8 only)	2 (2 per site)	254457-B21
Sun 64-bit SBus HBA	4 (2 per site)	254458-B21
Windows 2000 or Windows NT KGPSA-CB	4 (2 per site)	176479-B21

Table 33: Required Items (select one)

Description	Quantity Required	Part Number
Note: Refer to the DRM Release Notes for additional Fibre Channel switches that are supported. In addition to the B- and M-series switches listed below, C-series switches have been approved for use with DRM.		
B-series switches		
Fibre Channel Switch 16 port	4 (2 per site)	158223-B21
Fibre Channel SAN Switch, 8-port	4 (2 per site)	158222-B21
Fibre Channel SAN Switch, 8-EL	4 (2 per site)	176219-B21
Fibre Channel SAN Switch, 16-EL	4 (2 per site)	212776-B21
SAN Switch 2/16, 16-port, 2 Gb	4 (2 per site)	287055-B21
SAN Switch 2/16-EL, 16-port, 2 Gb	4 (2 per site)	283056-B21
SAN Switch 2/8, 8-port, 2 Gb	4 (2 per site)	258707-B21
StorageWorks Core Switch 2/64, 64-port, 2 Gb	2 (1 per site)	254508-B21
Optional Switch Rack-Mount Kit	4 (2 per site)	167365-B21
Optional Redundant Switch Power Supply (for 8- and 16-port Fibre Channel Switch)	4 (2 per site)	160407-B21
Extended Fabric License	1 per site	262868-B21
M-series switches		
StorageWorks SAN Director 64, 1 Gb	2 (1 per site)	254512-B21
StorageWorks Director 2/64, 64-port, 2 Gb	2 (1 per site)	286809-B21
StorageWorks Edge 2/32, 32-port, 2 Gb	4 (2 per site)	286810-B21
StorageWorks Edge 2/16, 16-port, 2 Gb	4 (2 per site)	286811-B21
Fibre Channel Switch, ES-3032	4 (2 per site)	order from vendor

Table 34: Fibre Channel Cables and GBICs MMF Cables

Description	Quantity Needed	Part Number
Fibre Channel Short-Distance GBIC	Minimum of 12 (half per site)	380561-B21
Fibre Channel Cable Kit (2 GBICs, two 2-m cables)	Minimum of 6 pairs	380596-B21
Fibre Channel Cable Multimode (2 m)	Minimum of 6 pairs	234457-B21
Fibre Channel Cable Multimode (5 m)	Minimum of 6 pairs	234457-B22
Fibre Channel Cable Multimode (15 m)	Minimum of 6 pairs	234457-B23
Fibre Channel Cable Multimode (30 m)	Minimum of 6 pairs	234457-B24
Fibre Channel Cable Multimode (50 m)	Minimum of 6 pairs	234457-B25

Order a minimum of 6 pairs of MMF cables and 12 GBICs and ship half per site.

glossary

This glossary defines terms used in this guide or related to this product and is not a comprehensive glossary of computer terms.

asynchronous transfer mode (ATM)
A mode of operation of the remote copy set where the write operation reports command completion to the host after the data is on the initiating controller, but before completion of the remote command.

This communications networking technology for LANs and WANs carries information in fixed-size cells of 53 bytes (5 protocol and 48 data).

See also synchronous mode.

bidirectional DRM
A tested set of storage hardware and software products configured to allow two sites to use each other to maintain synchronized remote copies of online data.

constant bit rate (CBR)
Category of ATM service that supports a constant or guaranteed data rate. CBR supports applications that need a highly predictable transmission rate.

data rate
The amount of data transferred per second by a communications channel, computing device, or storage device.

default gateway
The default path that a computer or router uses to forward and route data between two or more networks that have different protocols.

disaster-tolerance (DT)
The capability for rapid recovery of user data from a remote location when a significant event or disaster occurs at the primary computing site.

dual-switch/single-site
A complete storage offering based on the DRM dual-switch/single-site for the Windows NT solution that provides the highest level of data availability in single-site environments. Based on switched fiber, this solution enables a customer to pinpoint and support a critical application and to scale up as that application grows or new applications are added.

E1
The standard European carrier for transmission at 2.048 Mbit/sec.

E2
The standard European carrier for transmission at 8.192 Mbit/sec.

E3
The standard European carrier for transmission at 34.368 Mbit/sec.

E4
The standard European carrier for transmission at 139.264 Mbit/sec.

E5
The standard European carrier for transmission at 565 Mbit/sec.

fabric
A network of Fibre Channel switches and attached devices.

Fibre Channel (FC)
Technology for very high speed, switching-based serial transmissions.

Fibre Channel Arbitrated Loop
A serial data transfer protocol developed by storage device manufacturers and standardized by ANSI in which high-bandwidth transfer is accommodated between SANs. FC-AL supports optical media and supports full-duplex transfer rates between SCSI storage systems.

FC-IP
A configuration in which Fibre Channel Protocol data is transmitted via an Internet Protocol intersite link.

gigabit interface converter (GBIC)
The hardware devices inserted into the ports of the Fibre Channel switch that hold the Fibre Channel cables. GBIC devices are available for short-range applications (0.5 to 500 meters), long-range applications (up to 10 km), and very long distances (up to 100 km).

gigabit link module (GLM)
A device (permanently installed) that provides fiber-optic cable transmission at distances of 0.5 to 500 meters, depending on the cable size and quality of its installation.

hop
One interswitch link.

initiator
For subsystems using the disaster-tolerant Data Replication Manager solution, the initiator is the storage array that is the primary source of information. In the event of a system outage, the database would be recovered by the initiator from the target system. The initiator site is also referred to as the local site.

ISL
Intersite or interswitch link. The acronym is context sensitive.

latency
The amount of time required for a transmission to reach its destination.

link
A connection between two adjacent Fibre Channel ports consisting of a transmit fiber and a receiving fiber. An example is the connection between the Fibre Channel switch port and the HSG80 controller.

MB/sec
Megabyte per second, sometimes shown as MBps.

Mbit/sec
Megabyte per second, sometimes shown as MBps.

MMF
Multimode fiber, typically 50 micron, although 62.5 micron is also supported at reduced distances.

OC3
The optical carrier that provides high-speed bandwidth at 155.3 Mbit/sec.

OSG
Open Systems Gateway. OSG converts Fibre Channel to and from ATM.

peak cell rate (PCR)
Peak cell rate is the maximum transmission speed of a virtual connection and is a required parameter for the CBR service category.

permanent virtual circuit (PVC)
Logical connection between two points that are manually defined by the network administrator.

quality of service (QoS)
The performance of the connection as measured by the established QoS parameter, which is outlined by the ATM forum. Each virtual connection in an ATM network has a service category.

redundancy
The provision of multiple interchangeable components to perform a single function to deal with failures and errors. A RAIDset is considered to be redundant when user data is recorded directly to one member, and all the other members and associated parity also are recorded. If a member is missing from the RAIDset, its data can be regenerated as needed, but the RAIDset is no longer redundant until the missing member is replaced and reconstructed.

SCSI (small computer system interface)
An American National Standards Institute (ANSI) interface standard defining the physical and electrical parameters of a parallel I/O bus. A processor-independent standard protocol for system-level interfacing between a computer and intelligent devices including hard drives, disks, CD-ROMs, printers, scanners, and other devices.

single-mode fiber (SMF)
A single-mode fiber, typically 9-micron, although 8- and 10-micron are also supported.

SONET (synchronous optical network)
An ANSI standard for transmitting bits over fiber-optic cable.

speed of light through fiber
Approximately 200,000 kilometers per second or 5 microseconds to traverse one kilometer.

synchronous mode
A mode of operation of the remote copy set where the data is written simultaneously to the cache of the local subsystem and the cache of the remote subsystem. The I/O completion status is not sent until all members of the remote copy set are updated.

See also asynchronous mode.

target
For subsystems using the disaster-tolerant Data Replication Manager solution, the target is the storage array that is the secondary or backup source of information. In the event of a system outage, the database would be recovered from the target system. The target site is also referred to as the remote site.

T1
The standard North American carrier for transmission at 1.544 Mbit/sec.

T2
The standard North American carrier for transmission at 6.176 Mbit/sec.

T3
The standard North American carrier for transmission at 44.736 Mbit/sec.

trunking
The combining of two or more low-speed links into one virtual high-speed link. In a Fibre Channel fabric, trunking means combining two or more intersite links (ISLs) into one virtual high-speed ISL.

unspecified bit rate (UBR)
Data transmission that offers no traffic-related service guarantees.

virtual channel (VC)
The field of the cell header storing the VC address.

virtual path (VP)
The highest-order logical address in ATM. VP refers to a given group of circuits on a link.

virtual path identifier (VPI)
The field of the cell header storing the VP address

VLD GBIC
Very long distance GBIC.

wavelength division multiplexing (WDM)
The ability to have multiple optical signals share a single optical cable.

index

W